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
Presented by Otsuka Corporation

BP Navigator

usiness artner

2003
第11号

巻頭特集

セキュリティ特集
今、そこにある脅威

BP Navigator
business partner

11

CONTENTS

日本のメーカを軸に『ユビキタス』が加速する

トレンドマイクロ株式会社
執行役員　日本代表
大三川 彰彦氏

お客様の現場で感じたトレンドマイクロのサポート能力

私は1982年に大学を卒業後、当時のDEC（現HP）に10年半ほど在籍し、代理店、OEM、エンドユーザ、ラージアカウントと、営業担当として経験を積ませていただきました。その第一線において、お客様がMSネットワークやパソコンのLAN等へ期待感を高めている状況を肌で感じ、新しいコンピュータネットワークの時代というものを予感しておりました。その後マイクロソフトからお誘いをいただき、1992年から約10年間、マイクロソフト社でWindows NTの立ち上がり、成熟、そして各種サーバ製品の誕生へと立ち会った形となります。

そして、ちょうど私がエンタープライズ営業の責任者をしていたときに、これまでに無いほどに進化した、コンピュータウイルス（ワーム）「コードレッド」や「ニムダ」の猛威を体験しました。マイクロソフト社員としてその対応に追われていたところ、お客様の現場において、トレンドマイクロの迅速なサポート対応を目の当たりにし、その存在を強くインプットされたのです。

日本代表への就任、そしてトレンドマイクロの第2フェイズへ向けて

2003年2月に、弊社スティーブ・チャンから「トレンドマイクロの第二フェイズを一緒に創り上げていこう」という誘いを受ける形で入社、その後、執行役員 日本代表に就任させて頂きました。トレンドマイクロは1989年にスティーブ・チャンがウイルス対策の専門会社としてアメリカで立ち上げた組織ですが、最終的に日本に本社を構え、ワールドワイドに展開を行い発展してきた会社です。日本に開発部隊を置き、日本のお客様の声をダイレクトに聞きながら育ってきたということは、お客様にとっても我々にとっても大変なアドバンテージだと考えています。

トレンドマイクロのこれまでの段階というのは、コンピュータウイルスの登場と、Windows95リリースによる爆発的なインターネット人口の増加という状況に対応するため、その瞬間を駆け抜けてきた15年間でした。しかし現在では、ウイルス自体もさらに強力なワームに進化していますし、市場的にもウイルス対策ソフトはその必要性を認められ、普及段階を終えています。そういう状況において、従来の“プロダクツ・アウト”という体制ではなく、“サービス”を供給する会社へと戦略的に移行しているのが現在の段階です。全世界6拠点の「TrendLab（トレンドラボ）」と呼ばれるウイルス解析・サポートセンターにおいて、24時間365日いつでも、全世界にウイルスパターンファイルを供給しているのも“サービス”ですし、『トレンドマイクロコントロールマネージャー』という管理ツールに連動して、ウイルス感染予防や感染後の自動後処理などを提供しているのも、他社にない“サービス”です。ITインフラを基本としながら“サービス”を提供する体制を強化していくこと。これがトレンドマイクロが迎える第2フェイズと考えております。

企業向け製品シェアNo.1と『4C+T』

弊社は「ウイルスバスター」の成功により、コンシューマ寄りのベンダーと認識されているお客様も多くいらっしゃいます。しかし実際には、日本はもちろん、世界においてもインターネットゲートウェイ（ウェブサーバ）対策製品市場でシェア1位、メールサーバ向けウイルス対策製品市場でシェア1位を占めるなど、企業向け製品の分野においても、市場的、ノウハウ的にも、またウイルス対策の技術面でも特許を持つなど、全てにおいてアドバンテージを誇っています。

例えば自らシステムを運用し、情報・セキュリティポリシーを確立しているような大企業や、ネットワークの運用までを自社で行っているような中規模の企業、専任の管理者が存在しないサービスプロバイダを利用して運用している小規模のオフィスまで、各カスタマー・セグメントごとにどのように“サービス”を供給するのが効率的なのか？どのようなパートナーと協力すれば各カスタマー・セグメントに訴求が可能なのか？といったように、戦略的に物事を考え、造りあげ、表現していく必要性を感じています。

今回弊社では『パラマウント』という社是を作り、“安全なデジタル情報を交換できる”というビジョン、“顧客のデジタル情報資産を守るリーダーになる”というミッションを掲げ、それを実現するための“Creativity（創造性）”、“Communication（コミュニケーション）”、“Change（変化）”、“Customer（顧客）”、“Trustworthiness（信頼性）”、この『4C+T』こそが弊社の価値であるというコンセプトを打ち立てました。企業向け、コンシューマ向けを問わず、我々の取り組み方をこのように積極的に明示してソリューション提供を行っていきます。

そんな中で、グローバルスタンダードである者同士が自分たちの専門分野を充分に発揮し、より良いソリューションを提供することで、相乗効果を狙い提携／展開していくソリューションとして『ベスト・オブ・ブリード』という展開を用意しております。例えば2003年5月22日に提携発表しましたように、VPNに特化しているネットスクリーン社と提携することで、その優れたハードウエア技術の上にトレンドマイクロのウイルス対策技術が搭載され、アプライアンスとして提供される、というようなパターンです。このように、SI&インテグレーターにベストなソリューション提供を実現するための展開を考えています。

大塚商会と協力して、さらなる企業向けコンシューマ向けソリューションの展開を図る

私としましては、『ユビキタス（即時性）』の鍵を握るメーカーが日本に揃っている、そしてまたトレンドマイクロも日本に本社を構え展開しているメーカーである、という環境・状況に大変興味を持っています。日本でのインターネット環境を考えると、初期の電話回線を利用した課金制ダイアルアップ接続から、現在では光ケーブルまでを含めた常時接続へと一挙に加速しています。そんな中で、当社ウイルス対策製品の即時的かつ自動的なアップデートはもちろんですが、より利便性を大きく打ち出したソリューションを、大塚商会様と協力しながら提供していきたいと考えています。また弊社の一般・個人向け総合セキュリティソフトの『ウイルスバスター2004』のように、「MSブラスト」等といった次世代型ネットワークウイルスの事前対策機能に加え、パーソナルファイアウォール機能やURLフィルタリング機能、迷惑メール対策機能を搭載するなど、コンシューマ分野においても即時性のあるソリューションを提供させていただきます。

また、昨今のウイルス対策への認識の高まりで、実際にお客様の相談に乗れる、知識のある窓口が重要だと再認識しました。そこでTCAE（Trendmicro Certified Antivirus Expert）や、TCSE（Trendmicro Certified Security Expert）という、営業やエンジニアの方向けの、ウイルス対策の資格認定制度の展開をすすめています。今後も社員教育分野や導入後のサポートの充実を含めた『安心感』を、大塚商会様と組んで提供していきたいと考えております。

トレンドマイクロは、プロダクツ、サービスを含め『素材』を提供しているメーカーです。ですから、最終的に取り扱っていただく販社のみなさま、販社の先にいらっしゃるエンドユーザのみなさまの声を理解している大塚商会ビジネスパートナー事業部様の『調理』が不可欠だと考えております。今後さらに協力を深め、更なる企業／コンシューマ向けソリューションの展開に取り組んでいきたいと思います。

特集

今、そこにある脅威

● 田中亘

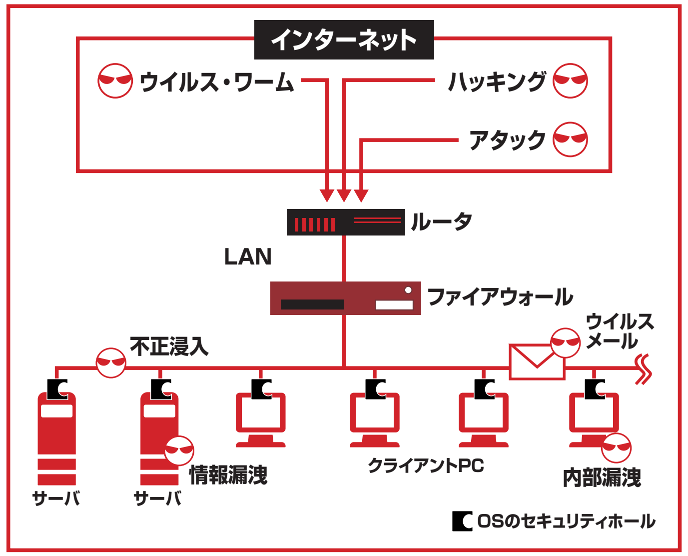
**いま個人も企業も、ITを取り巻くセキュリティに高い関心を示している。
それは、単なる興味や探究心ではなく、ITをインフラとして、ビジネス推進していく上においては、
必須の課題となっている。
これまで、日本は言語的な背景とネットワーク関連コストの高さなどが影響して、
海外との緊密なネットワークコミュニケーションがなかった。
それが幸いして、ネットワークセキュリティ関連の大きな被害からは遠ざかっていたが、
ここ数年のインターネットや電子メールの普及によって、
大手企業でも被害に遭う事件が増えている。
そうした背景から、ITインフラにおけるセキュリティの強化は、重要な投資課題となっている。
セキュリティにおける安全性を確保することが、
ひいては企業の信用にも関わる重要なテーマなのだ。
そこで、今回の特集ではセキュリティに関連するさまざまなチェック・ポイントと
対策について検証していきたいとおもう。**

企業情報システムにおけるセキュリティ・ポイントの概観

企業情報システムにおけるセキュリティ・ポイントの概観

一口にセキュリティといっても、情報システムを取り巻く危険性は複雑化している。ウイルスやハッキングは日常茶飯事に発生しているが、その他にも新たな脅威が我々の知らないところで起こり、それがインターネットを通して瞬く間に世界中に蔓延してしまう。また、外部からの脅威だけではなく、ネットワークの内側にもセキュリティの強化が求められており、情報漏洩や個人情報の保護などにおいて、社内における確固たるセキュリティの対策も必要になる。こうしたセキュリティ全般を取り巻くチェック・ポイントをまとめたものが図になる。

こうしてシステム全体におけるセキュリティのチェック・ポイントを総覧してみると、ウイルスに対する侵入検知は必須の項目であっても『それがすべてではない』ことがわかる。また、インターネットの普及当初には重要視されていたファイアウォールに関しても、いまでは当然の機能となり、そこからさらに踏み込んだ対策が必要になっているのも事実だ。



想定できる脅威と予期できない脅威

セキュリティを取り巻く脅威は、ネットワークの発展や個人の情報スキルが上がるにつれて増している。ネットワークへのアクセス/ログインなどの意味や目的がわからなかった頃には、さまざまなデータを手軽に取り出せるということが、どれだけ便利であるのか、そしてそれがどれ程の脅威であるのか、ユーザも管理者も気がついていなかった。むしろ、パスワードやアクセス権などを設定すると『アクセスがうまくいかない』など利便性を損なうことから、開きっぱなしの扉のように、オープンな利用環境が当たり前になっている例も多い。また、インターネットへのアクセスについても、ルーターの設定だけで精一杯で、ファイアウォールやパケットのフィルタリングにまで手が回らない中小企業もある。

確かに、セキュリティと利便性は反比例の関係にある。セキュリティを強化すれば、アクセスなどに認証やパスワードが必要となり、ユーザの使い勝手は悪くなる。また、認証や暗号化などのセキュリティを強化すれば、CPUやネットワークには負荷がかかっていく。それでも、想定される脅威と予期できない被害の損失規模を考えると、セキュリティに対する取り組みは必須だろう。実際に、利用者のセキュリティに対する意識も年々高まっている。ここ数ヶ月に開催されたセキュリティ関連のセミナーや展示会は、規模にかかわらず、そのどれもが満席や多くの来場者数を記録している。

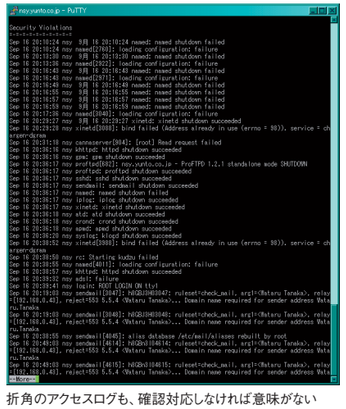
とはいうものの、実際に考えられる脅威がわからなければ、対応予算を組んで本腰を入れて対策に取り組むことはできないだろう。そこで、現在のところわかっている脅威についてまとめてみた。

10月22日～24日にかけて東京ビッグサイトで行われたセキュリティソリューション2003（主催：日経BP社）は、大塚商会を含む90社近い企業が参加し、近年のセキュリティ意識の高まりを反映して、連日大盛況であった

外部からの脅威

まず、外部からの脅威について考えみよう。最もわかりやすい意味で認識されている脅威といえば、やはりウイルスの侵入だろう。しかし、このウイルスも種類が多くなり日々進化しているので、その凶悪さによって被害も侵入経路も異なってきている。例えば、I love you ウイルスに代表されるメール型のウイルスでは、どんなに強固なファイアウォールや侵入検知を行っていても、個人のメールクライアントやメールサーバにメールとして入ってしまえば感染の危険が生じる。また、最近では被害が減ってきたとはいえ、相変わらずWordやExcelなどの文書に侵入して、マクロとして悪質なファイル破壊などを行うウイルスも未だ存在する。そして、最新型のウイルスでは、サーバやクライアントにあるセキュリティ・ホールを狙った攻撃をしかけてきており、このネットワーク型とか次世代型と呼ばれるウイルスは、これまでのワクチンソフトやウイルス検出ソフトでは対処できないという問題を抱えている。そのため、新たなウイルス対策が求められている現状だ。

一方、インターネットの中を乱れ飛んでいるハッキングや不正アクセスも後を絶たない。ルーターなどのログを見れば明確だが、毎日のように予期しないアドレスやサイトから、不正なアクセスを示すような痕跡が見て取れる。



折角のアクセスログも、確認対応しなければ意味がない

バッファオーバーフローの危険性

極端に考えるならば、バグのないソフトウェアはない。ソフトとして機能している以上は、何らかのバグを内包しているのは厳然とした事実だ。しかし、多くの利用者はそのバグに遭遇することなく、日常の業務をこなしている。そんな、ソフトの持つ脆弱性を悪用した不正アクセスが、バッファオーバーフロー攻撃といえる。

もっとも典型的な攻撃方法としては、ソフトのバッファ管理領域が容量オーバーで異常をきたす脆弱性を狙って、その弱みにつけこんだ攻撃を仕掛けてくる。通常の利用では問題の発生しないソフトであっても、悪意のある攻撃では動作に不具合が生じる。その結果、ハッカーは管理権限を乗っ取ってしまったり、ファイルの転送や書き込みなどを行い、ソフトそのものの機能を停止させるなど、ユーザに被害をもたらす攻撃を仕掛けてくる。こうしたバッファオーバーフロー攻撃の対象になるのは、これまではウェブサーバやメールサーバなどのサーバ系ソフトが多かった。しかし、最近ではクライアント用ソフトやOSの脆弱性を悪用し、同様の攻撃をしかけてくる例が増えてきている。それも、ハッカーなどの個人ではなく、ウイルスやワームの形で蔓延する悪質なものが急増しているのだ。NimdaやMSブラストに代表される悪質なワームなども、その攻撃パターンの中にバッファオーバーフローを悪用している。そのパターンはさまざまだが、いずれにしても対象となるサーバやクライアント、ひいてはそれを有する個人、または企業に多大な被害をもたらすものだ。

そして、内部からの脅威

セキュリティといえば、とかくウイルス対策にばかり注目がいきがちだが、個人情報保護法案などの影響によって、企業における情報漏えいなどに対するセキュリティの意識も高まっている。新聞やテレビにも取り上げられているように、いまでは社内のデータを不正に漏洩することも犯罪として摘発される。そうした事態が起きる前に、会社の内側にあるセキュリティ上の脅威を取り除く必要がある。ある意味で、働く人たちに罪を犯させないセキュリティを導入することが、情報管理者や経営者にとっての責任といえるのだ。そうした内側からの漏洩における脅威は、なんといってもパスワードのずさんな管理や、重要なファイルに対するアクセス権の未設定など、セキュリティ上での不注意なミスが多い。それに加えて、OSそのものの脆弱性を悪用する内部犯行の例もある。例えば、UNIX系OSではrootというユーザ名には特別な管理権限があり、このユーザとしてログインすれば、どんなファイルでも自由に閲覧できてしまう。また、一般のユーザでもsu(スーパーユーザ)コマンドとパスワードさえ知っていれば、root権限と同じ特権を行使できてしまう。

また、Windows系OSでも、ファイルやフォルダに対するアクセス権を設定していなかったり、ファイルシステム(ハードディスクフォーマット時に設定)をFAT32のままで運用していると、第三者や所有者以外の誰かに情報を盗まれる危険性もある。

ウイルスやハッキングといった外部からの脅威に加えて、これからのセキュリティ対策においては『内側の強化』も重要な課題なのだ。仮に、善良な社員ばかりの企業であっても、外部からの派遣社員や悪質なスパイなどが社内の端末を操作しないとは限らない。そうした不安を払拭するためにも、内側での万全なセキュリティ対策が求められている。

最新セキュリティ・ソリューション

『セキュリティ・ソリューション概観』

セキュリティを取り巻くさまざまな脅威に対して、実際にどのように取り組んでいけばいいのか。いま、その課題を真剣に受け止め、対策を模索している企業は多い。前のページで触れているように、一口にセキュリティといってもその範囲は広く、どこか一箇所だけを防いだとしても、別の場所から情報が漏れたり破壊される危険性は否めない。そのため、理想とはいえども『万全の対策』が求められている。

これだけあるセキュリティ対策

外部/内部のセキュリティに対する脅威から、すべての情報資産を守るためには、総合的なセキュリティ対策が求められている。そこで、先のセキュリティ・チェックポイントに対して、どのような対策があるのかまとめてみた。

まず、ウイルス対策ではワクチンソフトの導入が必須だ。ただし、最新型のワームは単純な「ファイルスキャン型」のウイルス検出だけでは、防ぎきることができない。ワーム型の攻撃を察知して対策を講じるためには、さらに進化したセキュリティ対策ソフトの導入が必要になる。具体的には、個々のPCにパーソナル・ファイアウォール(クライアントPCレベルで動作するファイアウォール)を設定し、システムを常にスキャンして不正なコードが実行されていないかを自動的に検査し、対策を講じるソフトの使用が必要だ。

また、不正アクセスに対する侵入検知は、個々のクライアント用PCへの導入に以上に、サーバやネットワークにも必要になる。サーバのファイルを常に監視して、システムやアプリケーション関連のファイルに不正なアクセスや改ざんがあれば、すぐに復旧を試みたり、ネットワークを監視していて、異常なパケットやトラフィックが発見されたら、その回線を論理的に切断するなどの処置を行う「監視&対策」ソフトが必須だ。より積極的なセキュリティ対策にとっては、検出するだけではく『処置を行う』ことが重要なのだ。

ある意味で、セキュリティ上の脅威に対してのシステムの停止や回線の切断は、かなり高度な経営判断を求められるといえるだろう。そのため、ソフトウエアによる処置対策と併せて、ネットワーク緊急時の対処などをまとめた命令指揮系統マニュアルの整備も重要な課題だ。

ウイルスやワームに不正アクセスへの対策に加えて、ファイルなどの情報資産を確実に守る方法が、暗号化と認証になる。つまり、サーバに保管するファイルそのものを暗号化してしまって、正当なパスワードを持っている者だけしかファイルを開けないようにすれば、万が一ファイルが盗み出されても情報は漏れない。Windows系のサーバOSにも、ファイルを暗号化する機能は備わっているが、より安全で確実なセキュリティを心がけるのであれば、第三者の認証機関によって管理されている認証キーと承認サーバの組み合わせを導入することが理想となる。そして、社員全員にIDキーを持たせて、OSで利用しているユーザとパスワードに加え、認証キーを使ったログインを行えば、さらに安全性は向上する。

この認証キーによる安全な認証方法には、他にも指紋やICカード、USBキーなどを使う例もある。Windows系サーバOSでは、指紋認証デバイスやICカード読み取りデバイスなどをサポートしているので、個人の使うPCに組み合わせて、確実な個人認証を行うシステムを構築し、不正ログインやアクセスを防いでいる導入事例もある。

さらに進化したセキュリティ対策

インターネット先進国の韓国で開発され、日本ではミラクル・リナックス株式会社が取り扱う「MIRACLE HiZARD V2.5 for Linux(MIRACLELINUX版)」(ミラクルハイザード)は、外部からの不正アクセスや内部からの情報漏洩に対して、サーバを守るソフトウエアだ。内部や外部からの不正侵入を強力に防御する最先端のIPS(不正侵入防止システム)セキュリティソフトウエアで、オープンシステムの中核となった Linux, UNIX, Windowsの各種プラットフォームに、最先端のセキュリティ技術を付加し、運用性を劣化させ

ることなく、信頼性、安全性を強化する。これまで解説してきた侵入検知や認証システムよりも、さらに進化し積極的に働くセキュリティ対策として注目されている。その主な特徴は次のようなものだ。

1.アンチハッキング機能により乗っ取りを防御

既知の攻撃はもちろん、未知の攻撃やバッファオーバーフロー攻撃を強固に防御して、攻撃事象と防御したことを直ちに管理コンソールへ通知する。その結果、未対応のセキュリティホールが発見されたときにも、修正パッチが適用されるまでの隙に行われる攻撃を防ぐことが可能になる。

2.扱いやすく強固なアクセスコントロールで情報漏洩を防御

ファイルシステム、デバイス、プロセスに対するアクセスコントロールを、OSレベルで制限し、監視機能を強化する。OSの最上位のシステム管理者であっても読み書きができないように設定ができ、またRBAC(ロールベース・アクセスコントロール:役割によるアクセスコントロール)によって、容易にアクセスコントロールを管理できる。

3.GUI管理ツールによる容易な操作と帳票出力の提供

MIRACLE HiZARD Manager によりGUI管理コンソールから複数台のサーバに対してアンチハッキングの設定、RBACの設定など、様々な設定を容易に行える。さらに、MIRACLE HiZARD Managerと各サーバ間の通信は暗号化され第三者による傍受を防いでおり、MIRACLE HiZARD Reporterにより、GUIを通して運用管理報告書も自動作成できる。

4.主要アプリケーションとの連携動作検証

Webサーバ「Apache」・「PHP」と「Oracle9i Database」をはじめとする、主要なソフトウエア製品やファイルサーバの機能をもつ「Samba」などのオープンソースのソフトウエアとの連携動作検証を行い、既存環境にそのまま追加して利用できる。

常にシステムを更新するセキュリティホール対策

拡大するセキュリティの脅威において、いま最も危惧されている問題がセキュリティホールだ。ソフトウエアの不具合だけではなく、開発段階では気が付かなかった、設計や仕様によるセキュリティホールは、悪意のあるハッカーやワームにとって格好の標的になってしまう。その種類にも、バッファオーバーフロー型の脆弱性であったり、単純なプログラムミスによる抜け穴だったり、製品の仕様による必然的な通り道だったり、様々だ。こうしたセキュリティホールに関係する問題を解決するためには、とにかくシステムやアプリケーションを最新版にアップデートするしかない。新たに登場してくるワームやハッキングに対して、最新の対策を施すことが最善の防御となるのだ。

マイクロソフトでは、安定したソフトの利用を実現するために、常に最新のアップデートをWindows Updateというサイトからダウンロードできるようにしており、新しいセキュリティホールが発見されれば、すぐに最新のパッチを提供してくる。また、OSのバージョンによっては、アップデートを自動的に行うこともできる。

しかし、いくら自動化されているとはいっても、社内すべてのサーバやクライアントで、自動アップデートを行うのはかなりの手間だろう。ダウンロードまでは自動化されているが、そこから先のインストールは個人の判断に委ねられているからだ。そのため、ベンダーの中には自動アップデートをサービス&サポートメニューとして提供している例もある。さらに、OSベンダーの提供するアップデートに頼らずに、サードパーティ製品のセキュリティ対策ソフトを導入するソリューションもある。先に猛威をふるったMSブラストという新世代のウィルスにおいても、セキュリティ対策ソフトを導入していたPCでは、OSの脆弱性を攻撃されても防ぎきったという実績がある。いずれにしても、安全なシステムの運用を心がけるのであれば、セキュリティに対する万全の対策が求められる。

セキュリティ・ソリューション一覧

- ワクチン
- ファイアウォール
- 侵入検知
- 認証(指紋,ICカード,etc..)
- 暗号化
- システム(サーバ)監視
- OSアップデート
- VPN

セキュリティ・ポリシーへの取り組みと内部監査の重要性

『セキュリティ・ポリシーへの取り組みと内部監査の重要性』

安全で快適なITインフラの構築と運用にとって、いまやセキュリティ対策は必須のテーマとなっている。先のパートで触れた個々のセキュリティ対策も、個別に導入していくだけでは意味がない。それぞれの場面や目的に合わせた最適なソリューションの組み合わせ、つまりセキュリティ・ポリシーの策定が求められている。セキュリティに対する総合的な取り組みとして、情報セキュリティ対策推進室の策定する情報セキュリティポリシーを参考に、その取り組みと内部監査の重要性についてまとめてみた。

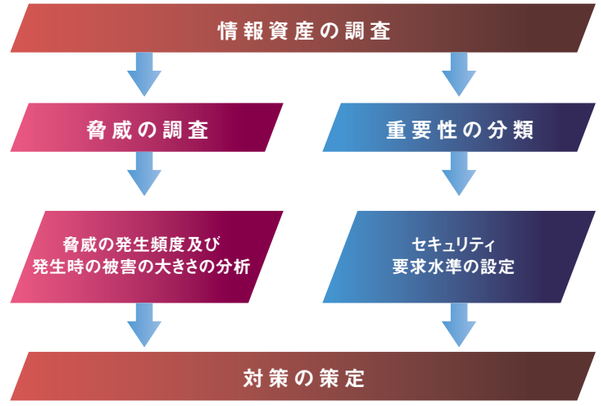
情報セキュリティポリシーとは

情報セキュリティポリシーは、平成12年に内閣安全保障・危機管理室と情報セキュリティ対策推進室が作成した、情報セキュリティを確立するためのガイドラインだ。それは、ウイルスなどによる被害だけではなく、情報そのものを安全に守るためのセキュリティ確保を目的としたもので、次の四つの観点に対する対策を目的としている。

①物理的セキュリティ
　施設・設備を保護する出入り管理等
②人的セキュリティ
　職員に対する教育・訓練、パスワード管理等
③技術的セキュリティ
　ネットワーク管理、ウイルス対策等
④運用
　システムの監視、緊急時対応計画の策定

情報セキュリティポリシーでは、管理指針(ポリシー)の策定を基本として、その導入から運用、そして評価を行い、見直しによるセキュリティ水準の維持を目指すものとなる。

また、平成13年には財団法人 日本情報処理開発協会によって、情報セキュリティマネジメントシステム(ISMS)適合性評価制度も創設されている。同制度は、平成12年度末に廃止された情報処理サービス業情報システム安全対策実施事業所認定制度(安対制度) に代わり、民間ベースによる第三者認証制度として位置付けられている。平成14年4月1日からの本格運用では、パイロット事業における対象範囲の業種制限を外し、全産業分野を対象としている。すでに、積極的なセキュリティ対策を導入しているデータセンターやSIベンダーの中にも、このISMSを取得している企業は多い。



ISMS適合性評価制度が立脚している規格は、「JIS X 5080:2002(ISO/IEC 17799:2000)情報セキュリティマネジメントの実践のための規範」になる。この規格は、組織の規模を問わず、情報資産を保護する必要がある場合に、情報セキュリティの範囲を明確にする際の枠組みや規範、基準になるべき考え方などをまとめたものであり、情報セキュリティマネジメントに対する普遍的、包括的なガイドとなっている。

このように、セキュリティに対する取り組みとしては、第三者認証制度もあり、政府レベルでのポリシー策定も提唱されている。そのため、これらの規範を元にして自社のセキュリティ対策を策定していくことで、最適で安全な運用を比較的容易に実現させることが可能だ。

重要な意味を持つ内部監査と再評価

セキュリティの対策において、過去にも現在にも、そして将来においても、永久に「万全」という技術はありえない。どんなに強固な守りを固めたとしても、悪意のある人間が作り出すセキュリティの脅威は、技術の進歩や情報の普及によって、より凶悪でさらに脆弱な箇所を狙った攻撃に発展していく可能性が高いからだ。そこで、情報セキュリティポリシーでも、ISMSの規範においても、セキュリティに対する内部監査と評価、そして改善というサイクル活動を重視している。

そのサイクルは、次のような流れになる。

Plan：情報セキュリティ対策の具体的計画、方針を策定。
Do：計画に基づいて対策の実施・運用。
Check：実施した結果の監査。
Act：経営陣による見直しを行い、改善。

この一連の流れを正確に処理するためには、先に触れている物理的・人的・技術的なセキュリティを確実に記録し監査する仕組みが必要になる。誰かがアクセス権を設定し忘れた機密ファイルにアクセスしていないか？、一般ユーザが管理者権限になりすましてアクセスしていないか？、不正なログやアタックが行われていないか？、そういった状況をすべて記録して、評価する仕組みが必要になる。いままでの一般的なセキュリティに対する取り組みといえば、その多くが技術的なセキュリティ対策が中心で、「外部からの脅威」を想定したものが多かった。しかし、これからは個人情報保護法案などの影響もあって、企業として「情報セキュリティ」に対する取り組みと姿勢が問われることになる。そのセキュリティにおける信頼性と安全性を強固なものにしていくためには、内部監査という視点でのセキュリティ対策も求められてくる。

キーワードはアクセスコントロール

内部監査を行うためのセキュリティ対策におけるITは、アクセスコントロールというテクノロジーに集約される。それは名前の通りに「アクセス」に対する制限や制御を行う仕組みだ。前述した、UNIX系OSでのroot権限の不正取得などがそれだ。こうしたOSの脆弱性を守るためには、OSのユーザ権限よりも強固なアクセス制御を導入しなければならない。そして、実際の運用面においても、セキュリティポリシーを管理し設定するスタッフと、システム管理を行うスタッフを分けるなど、人的な配置による安全性や、人に罪を犯させないようにする体制作りが重要になる。つまり、通帳と印鑑を別々に保管しておくように、セキュリティの運用者とITシステムの運用者を分けることで、二重のチェックと予防が可能になるのだ。

アクセスコントロールによる内部監査では、正確なアクセスログも収集できるので、社内の誰がどのようなデータにアクセスしたか、あるいはしようと試みたかなどの形跡もすべて掌握できるようになる。そうしたログを分析し評価することによって、さらなるセキュリティ対策の改善や見直しが可能になる。また、顧客のデータを預かるホスティングサービスやデータセンターなどでも、依頼先の企業から信頼を得るために、内部監査の徹底は重要になる。どんなに信頼できる社員を有する会社であっても、情報システムには外部の人間が関わるケースが多い。特に、開発やメンテナンスなどを外部に委託している場合には、外部の人間が大切なデータにアクセスする心配もある。そして、それ以上に、社内的にもアクセスコントロールやログの収集を行っていることを明確にすることで、社内/社外を問わず、各個人に対する暗黙の抑制効果も期待できるのだ。

こうした内部監査の重要性は、顧客に対するセキュリティ対策の提案にとって、大きなポイントとなる。他社がウイルスや侵入検知のソリューションだけを提案しているとすれば、内部監査というセキュリティ対策の提案は、重要な付加価値となる。また、結果的に内部監査とアクセスコントロールの強化は、外部からの意図しないハッキングや不正アクセスに対しても、効果の高い予防策となる。

セキュリティには、冒頭で触れているように、物理的・人的・技術的予防と運用という4つの側面がある。このすべてがトータルにバランスよく管理され徹底されていなければ、本当の意味での安全は確保できない。そういう意味で、真のセキュリティ・ソリューションとは、単なる箱や物のセールスではなく『コンサルティングやサポート&サービスも含めたトータル・ケア』が重要ということにほかならない。それは考えてみると、ITシステムベンダーやリセラーにとって、大きなビジネスチャンスといえるだろう。つまり、セキュリティ・ソリューションの提案にとって、セキュリティに対する脅威と、それに対する防御の認識や意義をユーザに高めてもらうことが、もっとも有効かつ効果的なアプローチといえるのだ。意識が高まっているセキュリティ対策であるだけに、そこから真に顧客に信頼されるソリューションへと提案を深化できれば、堅実なビジネスへと発展していくだろう。

大塚商会のセキュリティ・ソリューション

大塚商会の提唱するOSM（Otsuka Security Management）は、企業のセキュリティをトータルにサポートします。OSMでは、最新情報に基づいた継続的なシステムの監視・保守・診断やセキュリティポリシーをベースとする社内教育の徹底など、トータルなサポートサービスです。大塚商会は、これまでセキュリティ導入のコンサルティングから、個別の運用・管理対策まで、多彩な企業のセキュリティシステム構築とサポートを手がけてきました。その知識と経験をもとに、あらゆる企業のシステム規模に合わせた、最適なセキュリティシステムを実現します。

ソリューション一覧

Data Backup	コンテンツフィルター Web用	アウトソーシング・監視サービス
Web改ざん対策	ファイアウォール	サーバクラスタ
デスクトップ監視	無線LAN	ウイルス対策
コンテンツフィルタ Mail用	IT資産管理	VPN

これからのセキュリティ対策

『情報セキュリティへの継続的な取り組み』

情報セキュリティポリシーに関するガイドラインでは、その対象範囲を「情報システムなど」と「情報システムに記録される情報」、そして「これらの情報に接するすべての者」と規定している。つまり、セキュリティ対策にとって、人的な要素が影響する範囲はかなり広いものといえる。ネットワークが普及し、企業内でもイントラネットやインターネット接続、そして電子メールのやり取りが日常茶飯事になってきた今日にあって、あらゆる人たちがセキュリティにおける被害者になる可能性を持つと同時に、加害者にも鳴りうる危険性も秘めている。そうした情報セキュリティに対する継続的な取り組みを行うためには、改めてそのポリシー策定と管理サイクルの徹底が重要になってくる。

セキュリティの再確認

もう一度セキュリティに関係する管理のポイントを整理しておこう。

① 物理的セキュリティ
データセンターや情報システム部門のある企業では、サーバルームなどに鍵がかかっていて、IDカードや指紋認証などで出入りすることが当たり前になっているが、一般企業では施設や設備の出入りに対する管理や保護が徹底されていないことも多い。これらのソリューションは、警備会社などの担当になる面も多いが、情報セキュリティ対策にとっては重要なポイントとなる。

② 人的セキュリティ
物理的なセキュリティだけでは防ぎきれない問題が、社員や出入りする人たちに対する意識の徹底だ。パスワードを書いた紙をモニタに貼っていたり、ログインIDと同じパスワードにしているなど、人の心の油断や隙が、思わぬ情報漏洩につながる危険性がある。こうした部分は、社員教育やセキュリティ対策指導などによって、全社的に徹底していくことが有効な手段となる。

③ 技術的セキュリティ
一般的には、ITによるセキュリティ・ソリューションといえば、この技術的な側面が中心になる。これまでに解説してきた、システムやネットワークの監査や侵入検知に、ウイルス対策やファイアウォールの設定など、ソフトウエアやハードウエアによる「守り」のソリューションが中心になる。もちろん、技術的に優位に立っているセキュリティ・ソリューションを導入しなければ、日々発生する脅威からシステムを守ることはできない。そして、その優れたテクノロジーを最大限に活用するためにも、確固たるセキュリティポリシーの策定が求められている。

④ 運用
犯罪を発生させないために、警察や警備会社があるように、セキュリティ対策の徹底にとって、運用面での対策は最も重要な課題となる。特に、システムの監視と緊急時の対応計画は、経営や企業の規模に関わらず、必須のテーマといえる。ウイルスに感染したシステムから外部への被害を出さないために、ルータの回路を切断したり、メールサーバからの送受信をすべて停止するなど、緊急時の対策には高度な経営判断が求められる。こうした不測の事態において、冷静に対処するためには、常日頃からのセキュリティに対する運用体制のポリシー策定がなければならない。

安全で快適なITインフラを目指して

ITを取り巻くセキュリティの脅威が、社会的に注目を集めている理由は、その存在の重要さにある。いまや、インターネットを介した電子メールやHTML,XMLファイルのやり取りは、日常的なコミュニケーションの手段として確立されている。それだけに、情報化社会のインフラとしての役割が重要視されてきているのだ。停電や水漏れが生活やビジネスに大きな影響を与えるように、ITインフラを取り巻くセキュリティの脅威も、深刻な被害を社会に引き起こす。

しかし、だからといって、なんでもかんでも強固に守ればいいというものではない。実印は金庫の中に入れるけれども、認印は入れておかないように、守るべき情報やネットワークにも重み付け（プライオリティの設定）が必要だ。情報資産に対する正確な試算や価値を見極めることで、何に対してどこまで強固にしていくべきなのか、その取り組み方や対処のための予算配分が明確になってくる。また、セキュリティを提案する立場にいるシステムインテグレータやソリューションプロバイダにとっても、相手企業の情報資産に対する数字的な評価は、かなり説得力のある資料となる。

いずれにしても最終的なゴールは、安全で快適なITインフラの構築と継続にある。そのためにも、情報セキュリティポリシーに基づいた「構築→運用→評価→改善（再構築）」というサイクルを実現することが、最も有効な対策であり、そのサポートを行うことが、セキュリティ問題に対する最善のソリューション提供なのだ。

ITと勝ち組みの法則

【しきい値とビジネス】

「しきい値」という言葉を耳にしたことがあるだろうか。統計や解析などで使われることの多い用語だが。一種の「境目」を表す数値だ。そんな「しきい値」という言葉を、実は二つの極端なソリューションで耳にした。『ビジネス・インテリジェンス』と『運用監視ツール』だ。方やITソリューションの上流系の最たるもの。もう一方は縁の下の力持ち的な存在だ。しかし、このITソリューションの両端に位置するテクノロジーには、興味深い共通点がいくつもある。そして、その共通点から出てきたキーワードである「しきい値」を制するものが、ITにおける新たな勝ち組みとなっているのだ。

第11回
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。最近ではビジネスモデルやサービスなど、経営とITが密接に関連した事例や記事を手がけることが多くなっている。

●ビジネス・インテリジェンス

ビジネス・インテリジェンス、いわゆるBIとは、膨大な業務データの中から経営やマーケティング、またはセールスなど、さまざまなビジネスの最前線で行われる意思決定を支援するためのテクノロジーだ。ひと昔前に流行した「紙おむつとビール*」に代表されるデータウェアハウスとデータ・マイニングがより進化して、多角的かつ高度な分析ができるようになっている。かつて、データウェアの構築(ハウジング)とその分析(マイニング)のテクノロジーが発達した頃は、まだまだ荒削りなものだった。初期のデータ・マイニングでは、データベースに蓄積されたデータをOLAPと呼ばれるキューブ状の三次元的なデータの集まりにして、そこからピボットテーブルなどを活用してデータの中に隠された傾向や問題を分析していたが、その分析には、ある程度の技術的な基礎知識や高度な応用力が求められた。そのため、なかなか使いこなせる人材が育成されずに、データウェアハウスそのものの存在が疑問視されたこともある。

しかし、ビジネス・インテリジェンスの登場がそれを救った。製品やソリューションにはいくつかの種類があり、すべてをひとくくりで扱うのは誤解もあるが、一般的なビジネス・インテリジェンスでは、基本的な設定を行っておくだけで、データの中から求めるべき傾向や問題を発見しやすくなる。例えば、ある量販系チェーン店が、店舗ごとに集計される販売POSデータを元に、ビジネス・インテリジェンスで分析をかけたとしよう。通常であれば、単なる店舗ごとの売上推移と比較しかレポートされないが、ビジネス・インテリジェンスというフィルターを通して分析すると、商品ごとの細かい推移を追跡できるようになる。

仮に、店舗Aと店舗BのDVDデッキの販売台数が同じだったとしよう。しかし、店舗Aと店舗BのAV接続ケーブルの販売数を比べたときに、店舗Aが倍近く売り上げていたとしたら、そこに何かの傾向や可能性を見出せる。もしかしたら、店舗AはDVDデッキの近くにAV接続ケーブルを展示しているとか、レジでAV接続ケーブルが目立つように商品宣伝をし

「紙おむつとビール」とは・・・

バスケット分析によるデータマイニングの象徴的な事例。アメリカのスーパーマーケットにおいて、週末に訪れる30代の男性は、紙おむつと一緒にビールを買う確率が高いという分析結果をもとにして、紙おむつとビールの売り場を隣接させ並べて陳列したところ、紙おむつ、ビールともに売上が向上した事例に由来する、同時購買のパターンのこと。転じて、そのパターンを解析するデータウェアハウス手法全体の象徴としても用いられる。(編集部)

ていたのかもしれない。その結果、他のチェーン店にも同様の販売アドバイスを送ることで、売上を伸ばせる可能性が見えてくる。

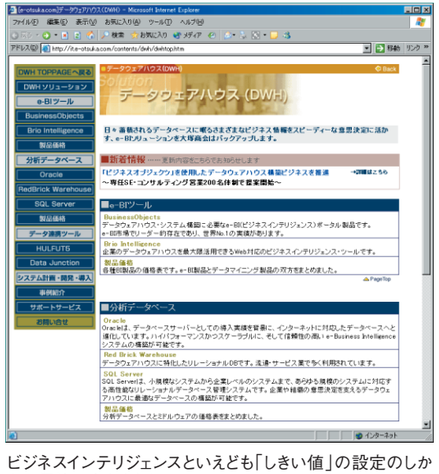
これは極端な例かも知れないが、変化する購買者の意識や傾向を理解するためのITとして、データの効率的かつ効果的な分析を提供するビジネス・インテリジェンスは、かなりの注目を集めているといえる。特に、大規模な店舗展開や販売を行っている分野では、すでに人知による全体の掌握が困難になっているだけに、ITによる解決策が重要視されている。

●ビジネス・インテリジェンスとしきい値

さて、データの抽出と分析に威力を発揮するビジネス・インテリジェンスだが、最近では「しきい値」によるダッシュボード化が進んでいる。例えば、業務における売上や在庫、借り入れや損金額など、注目しておくべき重要な数値に対して「境目」を設定する。在庫であれば、数量が5を切るとか、損金額であれば一部署で百万円を超えるとか、そういうポイントに注目して、収集したデータを常にモニタリングする。そして、実際に対象データが「しきい値」を超えたときに、メールや社内ポータルサイトなどを使って、担当者や経営者に「アラート」を発信する。それに気がついた担当者たちは、すぐに必要な対策を講じる。そうすることで、業務に支障をきたすことなく、円滑な意思決定とビジネスの継続を実現するのだ。

もちろん、在庫数などはビジネス・インテリジェンスを導入しなくても、その気になれば簡単に解決できるソリューションだろう。しかし、実際のビジネスの現場では、より高度で複雑な業務分析としきい値の設定が行われている。

先日取材したある商社では、各事業部ごとの業績を評価するために、個々の事業におけるリスク度とリターン率を算出し、収益性という評価でチャート化をおこなっていた。それは、商社というビジネス独自のノウハウを結集したもので、その結果として事業における投資価値や収益予測などを立てやすくなったという。同じように、国際的な部品調達を行っている製造業では、仕入れと歩留まりに関するビジネス・インテリジェンスを導入することによって、適正在庫や製造管理だけではなく、調達コストや生産効率などの改善を目指している。



ビジネスインテリジェンスといえども「しきい値」の設定のしかたで価値は大きく変わる
http://it.e-otsuka.com/contents/dwh/dwhtop.htm

こうしたビジネスにおける分析や統計によって、そこから導き出された「しきい値」こそが、その会社や業務におけるノウハウの集約であり、その値を上下させることが、現状のビジネスに対する大きな「改善」へとつながるのだ。

●運用管理としきい値

日本もPCの普及率がかなり改善されて、一般的な事務職における利用率は、かなり100%に近づいたのではないだろうか。むしろ、インターネットや電子メールがこれだけ当たり前に普及した現在において、いまさら導入していない企業というのは、その時点ですでに勝負を諦めているとしか考えられない。

しかし、PCを導入したらしたで、新しい問題も発生する。それが運用管理だ。

PCを入れた初期の頃というのは、誰もが故障とか修理とかを想定しているわけではない。自動車や複写機のような定期的な点検整備がないPCでは、いつかは壊れるということを考えずに、日々が過ぎていく。そしてある日突然に、ネットワークにつながらなくなったり、ハードディスクが動かなくなったり、電源が入らなくなったりする。そうした事態になってからはじめて、失ったデータの大切さや必要性に気が付くのだ。

こうしたトラブルに見舞われないためには、常日頃からの運用管理が重要になる。しかし、そこに人手はかけられない。そこで、運用監視系ツールが注目されている。それも、最新の高度な製品では、現時点での障害を報告するだけではなく、将来的な障害予測まで行う。その鍵を握るのが「しきい値」なのだ。

長年PCを使っていると、その機械が壊れることに何度も遭遇する。そして、壊れて動かなくなってから、記憶を辿ると「兆候」があったことに気が付く。例えば、ファンが壊れて熱くなっていたとか、ハードディスクから異音がしていたとか、ブートする度にビープ音が鳴っていたなど、新品の時にはなかった「兆候」があるものだ。そうした兆候を事前に察知しておくことができれば、壊れる前に保守できる。そうした障害予測を可能にするITソリューションが、運用監視ツールに凝縮されている「しきい値」になる。

●しきい値で勝ち組みになるとは

運用監視とビジネス・インテリジェンスは、テクノロジー的には類似したものだ。ある特定の数値に注目して、その数字の変化によって警告を出す。考えてみるとかなりシンプルな仕組みだ。しかし、その単純な仕組みの中にビジネスにおける勝敗を左右する重要な要素が隠されている。それが「しきい値」の設定なのだ。

もしも、安全で確実なビジネスや運用管理を行いたければ、警告を発する「しきい値」を高めに設定しておけばいい。早めの在庫補充や部品交換を行えば、欠品や故障の心配はなくなる。しかし、そうした安全策には「コスト」というリスクが伴う。

反対に、「しきい値」を下げておけば、在庫や部品のコストは削減できる。その見返りは「トラブル」というリスクになる。つまり、設定する「しきい値」によって、ビジネスにおけるリスクの配分が変化するのだ。リスクが完全に解消されることはない。一方のリスクを低くすれば、必ず対抗するリスクが高くなる。そのどちらの比率を変化させても、それは結局のところ「賭け」になってしまう。そうしたギャンブル的なリスクを避けるためには、両方のリスクが均衡となる「しきい値」を探し出さなければならない。そして、その値を探し出せた企業が、他社に勝る競争力を手に入れられるわけだ。

●最終的にはしきい値を超えた力を目指して

大塚商会ではハードウェアに限らず、各種監視ツールをソリューションとして用意している
http://it.e-otsuka.com/tkhn/solution/kanshi/kanshi01.htm

ビジネスとITを取り巻く「しきい」値は、リスクを最小限に減らすための努力であると同時に、ビジネスやシステムを正確かつ的確に分析するためのノウハウでもある。仮に、PCが壊れないと思って導入計画を立てる会社と、あらかじめ数年先には修理や買い替えが必要になると考えて予算を立てる会社では、投資に対するリターンの予測が大きく違ってくる。

そこには、明確になっていないものの、暗黙の「しきい値」が担当者の中にスキルとして蓄積されているのだ。その暗黙知を明確にする数学的な解決策が、「しきい値」の設定といえる。そして、その知識と経験を数値化してITの中に取り入れられた企業は、未着手の企業に対して競争で優位に立てる。

一方で、数値化された「しきい値」を提案することも、新しいビジネスとして成立するだろう。成功している事業や管理のノウハウというものは、その大部分がその「しきい値」の中に集約されている。それをパッケージ化して販売できれば、大きなアドバンテージになる。もっとも、単なる模倣ではNo.1になることはできない。基準となる数値から、どこまでオリジナリティを引き出せるかが、そのビジネスや管理における新たなノウハウであり、競争力の根源ともなる。そして、さらに理想を目指すのであれば、「しきい値」を超えたビジネスの継続や部品の保守を心がけるべきだろう。いい意味での「しきい値」に対する裏切りは、利益の増加や経費の節減につながる。監視やモニタリング系のシステムというと、とかく「管理されている」というイメージを与えがちだが、その反対に目標を超える努力を個々の社員や担当者に与えることができれば、さらなる成功も期待できる。

ビジネス・インテリジェンスや運用監視ほどの大規模で本格的な「しきい値」ではなくても、個人や部署やグループで、何らかの「しきい値」を設定する努力をするだけでも、ビジネスにおける大きな改善につながる可能性もある。いずれにしても、ITを効率よく効果的に使う目標の一つとして、「しきい値」に対する意識と取り組みは、勝ち組みになるための重要な要素だと考えられる。

今後の予定

- **サーチ力の違い、オークションとEC**
- **ライセンス料と保守サービス料**
- **セルフサービスで成功するビジネス**
- オープン・システムで話をする **三階層モデルとアプリケーション**
- 営業力を強化する **セールスフォース、eCRM**

…などなど

第4回　アドビシステムズ株式会社

ポイント制で自由に選べる 事業規模に応じて最適なプログラムが組める

アドビ・オープン・オプションズ・ライセンス・プログラム

数多くのデザイン・パブリッシング用アプリケーションをリリースするアドビシステムズ株式会社。そのアドビシステムズが提唱するライセンスシステムが「アドビ・オープン・オプションズ・ライセンス・プログラム」だ。このライセンスシステムは、各アプリケーションにポイントを割り振り、製品カテゴリーに関わらず、必要なライセンス数を自由に組み合わせができる方式を採用し、トータルで購入するポイント数が多いほど割引率が高くなるなどのメリットがある。教育市場向けのプログラムも用意されており、製品の導入や各種管理工数を軽減している。

必要な数、自由に組み合わせて ボリュームディスカウント

デザイン・パブリッシング用アプリケーション市場において、絶大なシェアを誇るアドビの製品群。個人事務所から中小～大企業まで、利用規模に違いはあってもそのユーザは多いはずだ。そんな全てのユーザを対象としたライセンスシステムが「アドビ・オープン・オプションズ・ライセンシング・プログラム」だ。

このライセンスシステムには大きく2つの括りがあり、一つは小～中規模の企業を対象とした「トランザクショナル・ライセンシング・プログラム（TLP）」、もう一つは中～大規模の企業を対象とした「コントラクチュアル・ライセンシング・プログラム（CLP）」だ。この2つのライセンシング・プログラムに共通のメリットは、アドビのほとんどの製品にポイント数が設けられていて、その合計ポイント数によってボリュームディスカウントが行われること。しかも製品のセレクトの仕方が自由なので、必要な製品を、必要な数だけ、組み合わせて選んでも、そのポイント数の合計を元に、無駄なくディスカウントが受けられる。

例えば、デザイン部門とデジタルビデオ制作部門、Web制作部門でそれぞれ購入していた異なるアドビ製品も、必要なライセンス分ずつまとめれば、それぞれ必要とする製品の数が多くなくても、効率良く安く購入することができる。また、プラットフォームごとに1つのシリアルで管理できるようになり、PCの買い換えや、ハードディスクトラブルによる再インストールの際などの管理を省力化することが可能で、インストールCDやマニュアルも必要な数量のみの購入で済み、製品パッケージ類の管理に、貴重なスペースを費やすこともなくなる。

少ない購入数でも利用可能な トランザクショナル・ライセンスプログラム

対象製品のポイント表と照らし合わせて、累計ポイントが5ポイントから1,000ポイント程度であれば「トランザクショナル・ライセンシング・プログラム（以下TLP）」がお勧めだ。今まで普通に販売店で複数のアドビ製品を購入していたユーザも割引を含めたTLPの各種恩恵を受けることができる。例えば個人事務所レベルでも、アドビ・イラストレーター、アドビ・フォトショップ、アドビ・インデザインの3種類のアプリケーションを1ライセンスずつ購入すれば、その時点で6ポイントとなりTLPの適用を受けることが可能だ。さらに、完全な新規購入でなくても、既に購入しているアプリケーションのアップグレードにも、アップグレードライセンス購入という形でポイントが加算されるので、アップグレード分、もしくは新規購入分と合計したポイント数でTLPを利用することができる。また「メンテナンスオプション」と呼ばれる最新アップグレードプログラム（適用2年間、購入条件あり）の購入にも、サービスを適用させるアプリケーションと同じポイント数が追加されるなど、導入の時の敷居の低さがTLPの最大の特長となっている。手続きも購入申込書を記入するだけなので、手軽でお得なライセンシング・プログラムといえるだろう。

主な対象製品 およびポイント

0.5ポイント	1ポイント	2ポイント	4ポイント
Adobe Acrobat® Elements	Adobe Photoshop® Elements Adobe Acrobat Standard Adobe Acrobat Professional 他	Adobe Illustrator® Adobe PageMaker® Adobe InDesign® Adobe Premiere Pro® Adobe After Effects® Adobe Photoshop® Adobe GoLive® Adobe FrameMaker® 他	Adobe Collections

※最新の対象製品ポイントはwww.adobe.co.jp/store/openoptions/で確認してください。

TLP
Transactional License Program

価格レベル	ポイント	価格レベル	ポイント
X	5−19	D	1,000−4,999
A	20−99	E	5,000−19,999
B	100−499	F	20,000−
C	500−999		

※教育機関向けは価格レベルAからになります

CLP
Contractual License Program

レベル	ポイント
D	1,000−4,999
E	5,000−19,999
F	20,000−

CLP
High Volume Discount

レベル	ライセンス数
K	1,000−4,999
L	5,000−9,999
M	10,000−24,999
N	25,000−49,999

※Acrobat製品のみが対象となります
※企業専用プログラムです
※HVDは1ライセンス単位の集計になります

※メンテナンスオプションはTLP/CLPの両方で適用可能です（プログラムによって細かい差異があります）

ポイント数集計は関連会社にまで コントラクチュアル・ライセンスプログラム

TLPが小規模事業者向けのライセンシング・プログラムとすれば、ポイント数1,000を超える購入者より適用されるのが「コントラクチャル・ライセンシング・プログラム（以下CLP）」だ。

CLPの場合、アドビと契約を締結し、契約期間中の購入目標が設定されるなど、適用規定は厳しくなる。その代わり、ポイント集計の適用範囲が、海外拠点を含めた全社および、50%を超える資本が入っている関連会社にまで広がるうえ、契約時の購入目標に応じて決定した価格レベルが2年間の契約期間、全対象アドビ製品に適用されるのだ。契約期間内であれば、1ライセンスから契約時の価格レベルでの追加購入ができるほか、アップグレードライセンス購入やメンテナンスオプション購入にも価格レベルの適用が可能だ。TLPの場合、ポイント数による価格レベルの適用が、購入の都度（トランザクションごと）に限定されているので、この点はCLPの大きなアドバンスといえる。また、過去に購入したライセンシング・プログラムやパッケージ製品からのアップグレードも一括して行えるので、ライセンスの統合と共に、管理者への負担を大きく減らすことができる。その他に対象製品をアドビ・アクロバットファミリーに絞った「CLP　ハイ・ボリューム・ディスカウント」プログラムも用意され、さらに求めやすい価格レベルの適用でアクロバットの導入を進められる。

教育機関向けには 同時使用ライセンス方式を用意

教育機関でアプリケーションを導入する際に問題となるのが、そのライセンス量の多さだろう。アドビシステムズを含め、多くのソフトウエアベンダーが教育機関向けには価格を抑え提供しているが、それでもトータルでの導入コスト高や管理の煩雑さから逃れられてはいない。そこでアドビシステムズでは、TLP、CLPともに教育機関向けのライセンシング・プログラム「TLP for Education」「CLP for Education」を用意。TLP for Educationでの最低取扱いポイント数が、通常の5ポイントから20ポイントに引き上げられているほかは、同じライセンシング・プログラムが適用されている。

ここで特筆に値するのは、物理的にインストールされるPC台数ではなく、物理的に同時に使用する最大ユーザ数をライセンス数とみなす「コンカレント・ライセンス」というメニューを用意している点だ。例えば、教育機関の視聴覚教室に導入したとしよう。4教室、100台のPCにアプリケーションがインストールされた場合、通常ならば、必要なライセンスは100だが、実際には1教室ずつでしか使用しないのであれば、同時に起動されるアプリケーション数を1教室分の25とみなし、購入が必要なライセンス数も25と設定する制度だ。これによってTLP、CLPのメリットに加え、アドビ製品を導入するためのコストを大きく引き下げることが可能で、導入を考えている教育機関にとって、多大なる福音になるといえるだろう。

求めやすいライセンスシステムこそが 違法コピーの最強の防止策

これらのライセンシング・プログラムを実施するにあたって、アドビシステムズでは「ユーザ側にわかりやすいライセンスシステムを用意することでソフトウエア管理にかかる各種負担を減らす」ことを最重要視している。なぜなら、実際に違法コピーなどで法的責任を問われる会社の多くは、一部の社員のセキュリティの不徹底などが元となり、管理者が知らないうちに、いつのまにか違法コピーが社内に蔓延していたというような、ライセンス管理の煩雑さや複雑さに起因するケースが多いからだ。TLP/CLPの導入で、より求めやすい値段で、よりクリアなライセンス管理を行うことこそが、違法コピーを防止する最強かつ最良の手段であるとアドビシステムズは考えている。

「国内パソコン出荷2桁増も手放しで喜べない理由」

JEITA出荷統計の正しい読み方

第9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、ビジネス誌、パソコン誌、ウェブ媒体などで活躍中。PCfan（毎日コミュニケーションズ）、ウルトラONE（宝島社）、月刊アスキー（アスキー）、PCWatch（インプレス）、ASAHIパソコン（朝日新聞社）、日経パソコン（日経BP社）で連載および定期記事を執筆中。また、エコノミスト（毎日新聞社）、プレジデント（プレジデント社）でも、IT関連記事を随時執筆している。近著に、「松下電器　変革への挑戦」（宝島社刊）など。

パソコン出荷台数を知るための公式データとして、業界内でよく利用されているのが社団法人電子情報技術産業協会（JEITA）が四半期ごとに発表しているパソコン出荷統計だ。

同統計は、デルコンピュータを除くほとんどの国内主要パソコンメーカーが参加している自主統計で、一般的に、市場全体の約90%をカバーしているといわれる。

その最新データとなる2003年度第2四半期（7〜9月）の出荷統計が先頃発表された。

これによると、国内のパソコン出荷は、台数ベースで前年同期比24%増の262万7000台、金額ベースでは同17%増の4030億円となり、台数、金額ともに2桁の大幅な伸びとなった。

2桁の伸び率を達成したのは、台数では2000年第4四半期以来10期ぶり。金額ベースでは、2000年第2四半期以来12期ぶりというもの。

国内の経済環境が回復基調に向かうとともに、景気低迷感が徐々に払拭され、企業の情報化投資、個人消費が上向き始めていたことが2桁増に達した背景だと同協会では分析しており、この好調ぶりを受けて、「今年度通期見通しである1020万台は、最低限の数字とし、さらに+αの出荷を見込みたい」と、事実上の上方修正を明らかにしたほどだ。

会見では、+αの具体的な数値については言及しなかったが、2001年度実績が1068万台であったことを引き合いに出し、「ここには到達したい」とコメントするなど、少なくとも4〜5%程度の上乗せを期待しているようだ。

しかし、市場動向や調査の背景などを見てみると、10期ぶりの2桁増を達成したとはいえ、実は、パソコン需要の本格回復とは言い難い状況にある。いや、むしろ、手放しで喜ぶのは危険だといわざるを得ない。

それにはいくつかの理由がある。

第1点目には、比較となる前年の第2四半期の出荷ベースが低いという点だ。

前年同期は、サッカーの日韓ワールドカップの開催によって、個人消費が低迷。パソコン出荷も同様に前年第2四半期実績は、前年同期比6.5%減の212万6000台と落ち込みを見せていた。昨年第2四半期を振り返ると、さらにその前年が20%台のマイナス成長となっていたことから、業界内では少なからず需要回復を期待した節があった。だが、結果としては、そこからさらに落ち込むという事態になったのである。

そうした意味で、今年2桁増の大幅な回復を果たしたとはいえ、残念ながら2000年度第2四半期の289万5000台には届いていないのである。

第2点目には、今年の場合の特殊事情として、各社のパソコン新製品投入が9月に集中し、9月だけの集計では前年同月比4割増と異例ともいえる伸び率を記録している点だ。これは当然、第2四半期全体の大幅な伸びを牽引する格好となっている。

例年ならば、9月は製品出荷を絞り込み、10月の新製品投入に控えるというのがメーカー各社に共通した戦略。しかし、今年の場合は、個人向けパソコンのリサイクル制度が10月1日から開始となったため、9月の駆け込み需要と10月以降の反動を懸念したメーカー各社が、PCリサイクルマークを貼付したパソコン新製品を前倒しで9月に出荷したという事情がある。

例年出荷を絞り込む時期に、出荷のピークを持ってきたのだから、4割増という数字も当然といえば当然である。

言い換えれば、年末商戦を含む第3四半期（10〜12月）のパソコン出荷量にも少なからず影響を及ぼすことになるのは間違いないだろう。

そして、3点目は今回の出荷統計からアロシステムが新たに参加している点だ。アロシステムは、パソコン工房などの店舗展開を全国規模で行う、ショップ系組立パソコンメーカーとして人気を誇る企業で、業界関係者などの声をまとめると、年間出荷台数は30万台程度と推定される。となると、同社が統計に参加するだけで前年比3%程度の上乗せ効果があるという計算だ。同協会では、前年に遡って上乗せして集計することがないため、前年第2四半期は17社の出荷統計、今年は18社の集計での比較ということになるのだ。

こうしたいくつかの要因を見ると、2桁増という高い成長率を達成したとはいえ、市況回復と断言するのはまだ早いといえるだろう。

むしろ、この2桁増をベースに今後の成長曲線を描くことの方が危険だといえ、パソコン需要の本格回復を判断するのは、個人需要が集中する年末年始商戦を含む第3四半期の動向、そして年度末の企業需要の動向を見てからになりそうだ。

今のショップに足りないもの

第11回 「ユビキタス時代のPCビジネスを推察する」●島川言成氏

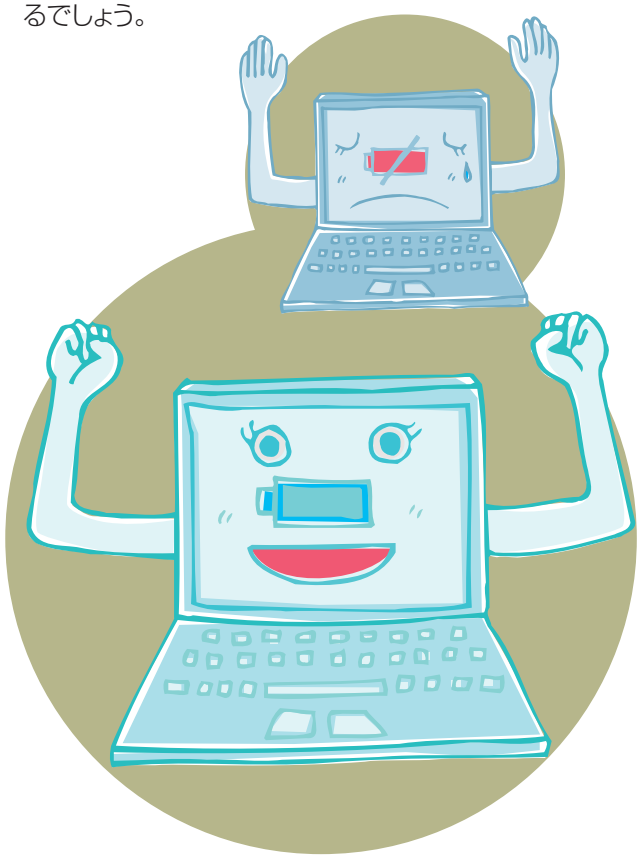
秋はPC関連のイベントラッシュが続きました。幕張メッセ、東京ビッグサイトなどで開催されたPC関連イベントを見学して、自分なりの結論を示しますと、業界はユビキタス環境を前提としたビジネスを模索しはじめているということです。ユビキタスは「いつでも、どこでも」とか「偏在」などと翻訳できます。この意味とPCビジネスを繋ぐものは多様にあります。

無線LAN、携帯電話などとの連携ソリューションを連想される人もいらっしゃるかと思います。事実、展示会ではそれらをテーマにしたブースが目立ちました。携帯電話のブースで主役になっていたのは、2001年10月からサービスが開始されていた第三世代携帯でした。先陣を切ったドコモの「FOMA」の場合、テレビ電話や映像配信などのソリューションを提案したにも関わらず、当初の加入者は15万人足らず。2002年4月にKDDIは「CDMA2000 1x」で現行世代の利用者の移行させ、12月までに400万台という契約台数を獲得しました。両者の明暗が分かれた原因は、採用した規格にあります。欧州や日本の通信会社が採用した「W-CDMA」は電波基地局を新たに設置する必要がありましたが、北米方式（CDMA2000）を採用したKDDIでは、第二世代との互換性を保ち、しかも既存設備の利用が可能だったのです。現在はFOMAの電波基地局整備も整うようになり、第二世代携帯で圧倒的なシェアをもつNTTドコモの市場獲得へのマーケティングが注目されています。

ユビキタス社会を支援する機器の存在も見逃せません。PCを前提にした場合、「いつでも、どこでも」にとって最大の問題はバッテリー駆動時間です。秋葉原ではインテルのセントリーノモバイルテクノロジーを採用したノートPCがよく売れています。懇意にしている店員に、その理由を質問しました。

「既存のノートパソコンの場合、ユビキタス的な使用を考えると、バッテリー駆動時間に不満がありました。セントリーノ搭載モデルと従来モデルを、その部分での比較説明すると、大半の人がセントリーノモデルを選択しますね」

フリーランスライターを職業にしていると、過去、何度もバッテリー駆動時間でハラハラした経験があります。取材に持ち歩くくたびれたトートバッグには、必ずACケーブルを入れています。バッテリー不足の警告ランプが光り出し、「AC電源を貸してください。電気料金を請求してもいいです」と某ホテルの喫茶室で懇願したこともありました。しかし、数年内にはこの問題を抜本的に解決してくれる技術が一般化しそうです。いうまでもなく燃料電池です。秋の展示会でも、いろいろなメーカーが燃料電池の提案をしていました。ユビキタス環境で利用するには、形状をさらに小型化する必要がありますが、大勢の見学者が「いつでも、どこでも」社会の実現に期待している『証』と言えるでしょう。



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、日経BP社運営のビジネスサイト「日経 SmallBiz」でIT業界の現状分析とユニークな提案をするコラムを連載中。PC月刊誌「日経ベストPC」では秋葉原のマーケティング状況をリポート。また、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。