

# BP business partner Navigator

## Up Front Opinion

トレンドマイクロ株式会社  
日本代表

大三川 彰彦 氏

顧客視点の徹底、パートナー様との  
協業強化によりさらなる成長へ舵をきる

株式会社シマンテック  
代表取締役社長  
シマンテックコーポレーション副社長

木村 裕之 氏

安全性と可用性を武器にパートナー様とともに  
より成熟したITインフラの構築を目指す

## 最新ソリューション情報

中堅・中小企業向けに心配・手間いらず  
オールインワンの簡単セキュリティ対策製品が登場!

## おすすめ製品情報

BPパーフェクト・チョイス/液晶モニター

巻頭特集

適切な情報管理が社会的信頼を高める!  
「情報管理」に万全を期すために  
社内を総点検する

2006 vol.26

Presented by Otsuka Corporation



**BP**  
business partner  
Navigator

6P

**Up Front Opinion**

トレンドマイクロ株式会社  
日本代表  
大三川 彰彦 氏

**顧客視点の徹底、パートナー様との  
協業強化によりさらなる成長へ舵をきる**

8P

株式会社シマンテック  
代表取締役社長  
シマンテックコーポレーション副社長  
木村 裕之 氏

**安全性と可用性を武器にパートナー様とともに  
より成熟したITインフラの構築を目指す**

**巻頭特集**

18P

適切な情報管理が社会的信頼を高める!

**「情報管理」に万全を期すために社内を総点検する**

33P

[大塚商会セミナーReport]

企業価値向上のための内部統制とは!

「日本版SOX法・内部統制ソリューション」セミナー

34P

[パートナー様向けWebシステム]

**『BPプラチナページ』の機能をまとめて紹介**

38P

[大塚商会のService&Support]

TPS-SHOP/α Web/エデュケーション/トータルαサポート21/データリカバリーセンター

42P

[Open Source Solutions]

**何でも相談、24時間対応、最新メディアを配送**

**Red Hat Enterprise Linux「Plus」シリーズの新サポート**

54P

[おすすめ製品情報]

BPパーフェクト・チョイス / 液晶モニタ

62P

[コラム] 業務改革・改善のためのIT活用とは ⑦ 田中 亘

**セキュリティとコンプライアンスに向けた取り組みの第一歩とは**

64P

[コラム] 売れるショップに売れる人 ⑦ 島川 言成

**現代に通じる近江商人の心意気**

65P

[コラム] ビジネストrend最前線 ⑦ 大河原 克行

**大手電機メーカーの相次ぐ社長交代、その共通項とは**

66P

[データ] **BP Navigator Market Report Enterprise編**

68P

[最新ソリューション情報]

中堅・中小企業向けに心配・手間いらず

オールインワンの簡単セキュリティ対策製品が登場!

トレンドマイクロ

70P

**ソフトウェアライセンス ⑩ アドビシステムズ株式会社**

78P

**BP事業部ソフトウェアカタログ**

81P

**BP Navigator Back Number / AD Index**

82P

[大塚商会グループ情報]

大塚商会のグループ会社をご活用ください!

# 顧客視点の徹底、パートナー様との協業強化によりさらなる成長へ舵をきる

トレンドマイクロ株式会社(以下、トレンドマイクロ)は、セキュリティを取り巻く環境の変化に対応した事業展開として、製品切り口ではなく、顧客ニーズを切り口とした組織体制、サービス事業を強化する方針を打ち出しています。そこで、同社日本代表の大三川 彰彦 氏に、日本のセキュリティ市場におけるトレンドマイクロの優位性や新体制の肝となるパートナービジネスについて語っていただきました。



トレンドマイクロ株式会社  
日本代表  
大三川 彰彦 氏

## ◎2桁成長を続ける強さの原動力はサポート体制と日本国内の開発力

トレンドマイクロのウイルス対策ソフトの売上は毎年、2桁の伸び率を続けています。昨年はグローバル市場全体で17%伸び、日本でも同じくらい売上が伸びました。ウイルス対策ソフトは、大企業はもちろんのこと中堅・中小企業でもすでに導入済みの企業が多いのではと思います。しかし、それにも関わらずウイルス対策ソフトの売上が増加傾向にあるのは、2003年くらいからフィッシングやスパイウェアによる被害が増えてインターネットの新たな脅威となってきたことが要因の一つとしてあげられます。

特にウイルス対策ソフトは、お客様にとって継続性が必須になりますから、長い目で見たときにお客様にとって信頼できるソフトメーカーであることが重要なポイントになります。その点、トレンドマイクロはサポート体制がしっかり確立しているので、電話対応の仕方やレスポンスの良さなどをお客様から高く評価していただいています。

さらにトレンドマイクロは、国内に専門の技術陣を揃えていますので、日本のセキュリティ環境の変化に迅速に対応したソリューションをいち早く提供することができます。たとえば、最近、日本では、Winnyを悪用するウイルスによる情報漏えいが大きな問題となっています。その対応としてトレンドマイクロは今年3月2日に、社内ポリシーでWinnyの利用を禁止している企業において、社内ネットワークでのWinny利用を防止するためのツールとして「アドバンス検索ツール」を「ウイルスバスター Corp. アドバンス」(および同サーバ版)に同梱して提供、すでに「ウイルスバスター Corp. アドバンス」をご利用のお客様にも、本ツールを無償でダウンロード提供するという発表を行いました。本ツールは日本国内で開発したものであり、日本のセキュリティニーズにいち早く対応できる態勢がトレンドマイクロの大きな強みとなっています。さらに今後は製品だけでなく、ウイルス対策製品の土台となるパターンファイルなども、日本で作成から検証までを行えるようにしたいと考えています。そうすることで、お客様に対してさらにスピーディな対応が可能になると思います。

## ◎高い技術力とネットワークセキュリティで法人市場で高い評価と実績を誇る

日本では「ウイルスバスター」の認知度が高いので、トレン

ドマイクロの製品はコンシューマ向け中心のイメージがあるかもしれませんが、トレンドマイクロ全体での製品別の売上高を見ると、コンシューマ向け製品の売上が占める割合は22%で、78%が法人向け製品で占められています。

また、トレンドマイクロは、インターネットゲートウェイの分野で、最初に技術特許を取得して製品を世に送り出しました。同分野の製品は北米、ヨーロッパ、アジア、そして日本でもNo.1のシェアをずっと維持しています。そのうえ、『Lotus Notes』や『Microsoft Exchange』に代表されるメッセージングソフトのセキュリティ対策の分野でも、トレンドマイクロの製品はグローバル市場でNo.1のシェアを誇っています。トレンドマイクロはもともと法人向け製品分野に強い力を持っており、特にネットワーク系のセキュリティ対策では他社に先駆けて優れた技術をもっています。2年程前にシスコシステムズと独占契約を結び、同社にOEM(Original Equipment Manufacturer:相手先ブランド製造)製品を提供しているのも、こうした背景があるからです。今年2月には新たなOEM製品もリリースしました。その意味では、トレンドマイクロのネットワークセキュリティ技術の高さが改めて証明されたと自負しております。

## ◎パートナー様との協業により新しい付加価値サービスをつくる

トレンドマイクロの米国におけるビジネス展開は大企業から開始し、その裾野を徐々に広げており、昨年からコンシューマビジネスにも力を入れるようになりました。米国市場での営業方法は主に、各企業のCIO(Chief Information Officer)に製品の技術的な説明をして、それを理解してもらったうえで製品を購入していただいております。また、専門家から直接サポートしてもらいたいという要望が圧倒的に多く、各企業とダイレクトにお付き合いするケースが多く見られます。

しかし、昨年秋にマイクロソフトの『Small Business Server』に、簡単にインストールできるセキュリティ対策製品をリリースしたところ、この拡販にはパートナー様の協力が不可欠になってきました。そのため、欧米ではパートナー様施策の重要性に気づき、ようやく力を入れるようになってきました。

一方、日本では、多くの企業がハードウェアやソフトウェアを含めてひとつのソリューションをワンストップで提供してほしいという要望が強く、以前からパートナー様との協業を

重視して取り組んでおります。現在では、パートナー様と一緒に新しい付加価値サービスをつくりあげるフェーズに入っていると思います。特にウイルス対策ソフトは、他のソフトウェアと違って、継続的なライセンスビジネスが見込めます。また、それに付随した管理ツールやレポートツールをプラスアルファしてお客様に提供することも可能です。その意味では、大塚商会様のパートナー様にとっても、メリットがあるユニークな商材だと思います。

## ◎コアテクノロジーとパートナー様の得意分野とで高付加価値の製品やサービスを提供したい

昨年、私どもの社長がエバ・チェンに替わり、「お客様に満足いただけること」を目的に、顧客の行動の違いを判断し、それぞれのニーズに応じたソリューションを提供できる組織編成を実施し、始動しました。今年はその結果がさまざまな製品やソリューションとなってリリースされる予定です。

ウイルス対策ソフトを企業のネットワーク環境に応じてカスタマイズしてほしいという要望をお持ちのお客様もいらっしゃいますので、今後は、そうした要望にもお応えしていきたいと考えています。また、ネットワーク上のさまざまなデータをモニタリングして、それに基づいた適切なセキュリティ対策をお客様にアドバイスするサービスなどにも力を入れていきます。いわゆるテクニカルな集合体であるプロダクトではなく、柔軟にカスタマイズが可能なバリューの高い製品を提供していきたいと考えております。セキュリティ管理ツールの一元化や、ログデータを収集してレポートするといったバリューを可能にできたのも、トレンドマイクロでは集中すべきところにリソースを投入しているからなのです。そうした私どものコアテクノロジーと、パートナー様の得意分野を組み合わせることで、バリューで勝負する次のステージへ進むことができると考えます。

お客様の要望を一番ご理解されているのは、大塚商会様をはじめとするパートナー様です。そのため、パートナー様が熟知しているお客様の意見を積極的に取り入れながら、大手企業や中堅・中小企業用にセグメント分けをうまく行い、パートナー様と一緒に付加価値の高い製品やサービスを提供していきたいと考えています。

# 安全性と可用性を武器にパートナー様とともに より成熟したITインフラの構築を目指す

今やビジネスのインフラともいえるITには、セキュリティとアベイラビリティの両立が強く求められています。しかし、ビジネスにおけるITインフラの重要性が高まる一方で、安全性との間には乖離が広がりつつあります。日本の企業の大部分を占める中堅・中小企業のITインフラの整備と今後の市場戦略について、株式会社シマンテック代表取締役社長の木村 裕之 氏にお話を伺いました。



株式会社シマンテック  
代表取締役社長  
シマンテックコーポレーション  
副社長  
木村 裕之 氏

## ○セキュリティとデータ管理の統合によりITインフラに 新たなビジネスソリューションを提供

現代は、情報と通信の社会が成熟しつつあり、ビジネスにとってITは不可欠になってきています。ITはわずか十数年で、ビジネスの基盤になるまで急激に成長してきました。大手企業であれば、必要な人材をそろえ、設備投資を行い、ITインフラを支える人や組織も整備されています。

しかし、まだまだ安全なITインフラが築かれていないといえる段階にないのが、ITインフラの現状です。ITをビジネスに生かしていくためには、やはり安全、安心で信頼性の高い堅牢な仕組みが必要です。

ITインフラとしての本来の役割と現状にはギャップが開いてしまっていると感じています。つまり安全性、信頼性を脅かすさまざまなセキュリティの脅威に対して、ITインフラとそれによって広がるネットワーク全体を、守っていくソリューションが強く求められています。これはシマンテックにとって大変大きなビジネスチャンスと捉えています。

シマンテックは、今年4月にベリタスソフトウェア社との法人統合を完了いたしました。セキュリティとアベイラビリティを融合し、堅牢なITインフラを構築するために、それぞれのお客さまの異なるニーズに対して、そのニーズに合わせたソリューションを提供することがミッションなのです。そのために日本に根付いた企業として、日本市場に足場を築くことが大変重要なことであると認識しています。

統合されたシマンテックが提供できるソリューションとして、たとえば、バックアップソリューション『Symantec Backup Exec』とシステムリカバリソリューション『Symantec LiveState Recovery』を組み合わせることで中規模のディザスタリカバリシステムを実現できます。また、もはや基幹システムともいえる電子メールについては、アーカイビングソリューションにアンチスパムのセキュリティを加えることで、電子メール全体を安全に利用できるソリューションの提供が可能になります。

IT環境は企業ごとに当然異なります。ITに関わるシステム全体を見て、シナジー効果が生まれるソリューションを提供していくことで、ITインフラ全体の安全性と信頼性の底上げを図っていかねばいけないと考えています。そして、多くのお客様にとってITを、より使い勝手の良いITインフラ

にして、安全で安心して利用していただきたいと思います。そのためには、今、導入ニーズの高い多くの中堅・中小企業のお客様への対応が重要になってくると考えています。

## ○日本市場の高いニーズに応えるため 人材と資力を投じてビジネスを展開

世界40カ国以上に渡って事業を展開しているシマンテックのビジネスにおいて、日本の市場は非常に重要な市場として位置づけられています。シマンテックにとって、日本市場は、アメリカに次いで世界第2位の市場であり、製品のサポート面や品質に対するお客様の要求や期待度が、諸外国と比較して非常に高いことが特長です。つまりサポート対応のレスポンスとクオリティが同時に求められているのです。こうした厳しい要求に応えるために、ワールドワイドの中では類を見ないほどの人材と設備を、テクニカルサポートに投資しています。

そのひとつとして2005年に、ワールドワイドのエンジニアリングセンターの下部組織として、「シマンテックジャパンエンジニアリングセンター」を日本に開設しました。このエンジニアリングセンターの開設により、日本語環境や国内ベンダーが提供している環境で検証済みの製品を、迅速に導入・利用できるというメリットが提供可能になりました。

## ○日本版SOX法対応として コンサルティングサービスを提供

また、最近の市場の動きとしては、2009年から施行されるという日本版SOX法についての、ご質問やご要望が増えはじめています。シマンテックでは、「日本版SOX法導入支援推進室」を設置し、日本版SOX法の導入準備を支援する「ITリスクアセスメントサービス」の提供を開始しました。これは、「セキュリティポリシーレビュー」、「アプリケーション脆弱性レビュー」など5つのコンサルティングを提供するものです。

現在のお客様の状況を見ますと、日本版SOX法に対して、「どんな対応が必要なのか」、「どう対処すればいいのか」というまだ模索の段階にあるようです。日本版SOX法への対応は、長い期間をかけた企業全体の機構改革になると見てい

ます。そこで、どのようにデータを取り扱ったらよいか、セキュリティの全体像はどうあるべきか、などの視点から、まず第一段階としてアセスメントという形のコンサルティングサービスを提供させていただこうと考えています。

## ○法人向けビジネスの強化で 大塚商会様とパートナー様に大きな期待

シマンテックは、将来的に法人向け製品の割合をおよそ75%くらいに高める目標を持って進めています。ですから、法人市場への期待には、非常に大きなものがあります。ほとんどの企業がITの活用を経営の戦略課題として位置付けておりますので、企業規模こそ違え、ITの重要度はまったく変わらないものと考えています。

市場の裾野が非常に広い中堅・中小規模のお客様には、それぞれの企業規模とニーズにあった、ITインフラを守るためのソリューションや、それを実現していくためのサービスを提供していくことが大切だと考えております。

そのためにも、日本全国の販売パートナー様にできるだけ多くの情報をご提供すべく、今後はさらに地方展開に力をいれてまいります。製品セミナーの全国展開や、さまざまなセールスツールのご提供、さらにはシマンテックとパートナー様をつなぐ、シマンテックパートナープログラムの本格的な整備も進めております。

もちろん当社だけで、サービスまでを含めたすべてをお客様に提供することはできません。シマンテックの社員数から考えても、できることには自ずと限界が生じてきます。お客様ごとの条件やセキュリティの段階に応じた最適なサービスを提供するためには、パートナーの皆様のご協力が今まで以上に重要になってくるものと考えています。とくに全国を網羅している大塚商会様のパートナー様とは、一緒に協働していくことの重要性をますます強く感じています。

シマンテックのセキュリティ製品や、バックアップを中心としたアベイラビリティの製品を中心に融合されたひとつのソリューションとして、大塚商会様とパートナー様との協業によって、これまで以上に全国に広く展開させていただき、安全なITインフラの実現を目指していきたいと考えています。

## 適切な情報管理が社会的信頼を高める！

# 「情報管理」に万全を期すために 社内を総点検する

個人情報保護法が完全施行されてから1年が経過した。しかし、スパイウェアをはじめとする新種のコンピュータウイルスが急増し、ウイルス感染したWinny使用による情報漏えいの事故、事件が続発している。そのため、企業の情報管理に対して社会から厳しい目が向けられている。さらに、日本版SOX法の施行が間近に迫り、適切な情報管理に基づいた内部統制の仕組みを早急に整備することが企業には求められている。この時期、企業は情報管理にどのように取り組むべきなのか。経済産業省の「企業における情報セキュリティガバナンスのあり方に対する研究会 報告書」における情報セキュリティ対策ベンチマークを参考にしながら、企業が取り組むべき情報管理のポイントをまとめた。

## 今なぜ企業内における情報管理が重視されているのか？

今やわれわれの経済活動や社会生活はITによって支えられているといっても過言ではない。しかし、電子化された情報の流通によって利便性が高まる一方で、個人情報の漏えいなどによる社会的な弊害も出てきた。そのため、情報管理に関する法制化が進み、各企業は法令を遵守した適切な情報管理を行うことが、社会的信用力を高める時代となっている。

### 企業の社会的な責務として 情報管理の重要性が高まる

現在、わが国では、e-Japan戦略に基づく世界最高水準のIT社会が実現しつつあり、ITの活用がビジネスの効率化・高付加価値化をもたらしている。たとえば、2005年4月から施行されたe-文書法では、これまで紙媒体での保存を義務付けていた帳票類について、一部の例外を除いて電子文書による保存を認めている。これにより、民間企業における帳票類の印字・流通・保存にかかるコストが大幅に削減され、企業間商取引の電子化がより一層推進されるようになった。

ところが、情報が電子化されたことによって、新たな問題も出てきた。すなわち、インターネットや外部メディアを使って情報の流通が可能になったことから、コンピュータウイルスの感染拡大、機密情報の流出といった新しいタイプのリスクが顕在化してきた。そのため、情報管理を適切に推進することが必要不可欠になっている。しかも、各事業者から盗み出された個人情報が売買されるようになり、その情報が詐欺事件などに悪用されるケースが急増してきた。その結果、不正アクセス禁止法や個人情報保護法などが新たに法制化されるに至った。個人情報保護法では、各事業所に個人情報の安全管理に対する監督責任が義務付けられ、個人情報を適切に取り扱っていない事業者には厳しい罰則が科せられる。さらに日本版SOX法では、

2009年3月期の決算報告から内部統制報告書の作成が義務付けられるようになり、内部統制が有効に機能しているか評価するために、基幹系データベースのアクセスログの収集などが求められている。また、ISMS(註)やプライバシーマークなど、社会的ベンチマークとしての情報管理の認証制度も浸透してきた。その結果、法律や国際基準に準拠した適切な情報管理を行っていない事業所は、社会的な信用を得ることが難しくなってきた。そのため、企業内における情報管理の重要性がますます高まっている。

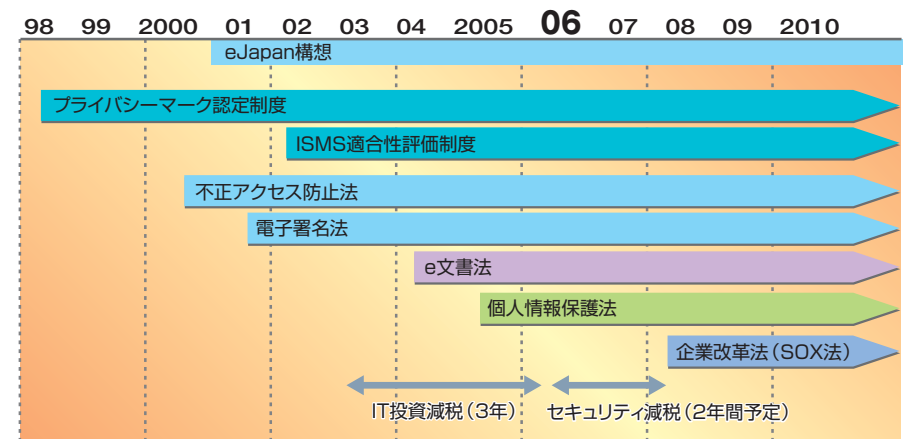
註) Information Security Management System＝情報セキュリティマネジメントシステム

### 法令遵守の情報管理の徹底は 社会的信頼と企業価値を高める

このように今や情報管理の必要性は、わが国の企業においても共通認識となりつつある。しかし、その実態は、

#### ■情報管理社会の進展

2000年以降、情報処理・管理に関する制度や法制化が進んでいる。IT機器を利用した業務効率化が進めば、ますます情報管理の重要性と整備の必要性は高まる。



コンピュータウイルス対策ソフトやファイアウォールといった製品の導入による対策が中心であり、セキュリティポリシーの策定やアクセスログの取得・解析といった社内組織的な対策は十分に行われていない状況にある。特に中堅・中小企業では、専任のシステム管理者が不在のケースが多く、情報管理が徹底しづらい状況にある。さらに昨今では、会社が支給したノートPCを自宅に持ち帰ったり、個人用のノートPCを会社に持ち込んで仕事をやるケースが増えており、組織的な情報管理がますます難しくなっている。

しかし、今や企業が適切な情報管理を行うことは社会的な責務でもある。むしろ、法令遵守の情報管理が求められる時代だからこそ、組織的な情報管理を積極的に行うことによって、顧客や取引先からの信頼度アップにつながるのだ。その意味では、情報管理の徹底は、社会的な信頼や信用を高める絶好のチャンスでもある。

## 運用管理ポリシーを人と組織に周知徹底させよう！

まず、情報管理ベンチマークの「運用管理要素」と「人的要素」からみた該当項目をチェックしていただきたい。もしもチェックできる項目が少なければ、経営層の情報管理意識が低いと考えられる。以下のポイントを参考にしながら、早急に情報セキュリティ対策を見直し、全従業員に周知徹底を図りながら確実に実践していくことが望まれる。

### 経営者が責任をもってコンプライアンスの推進体制を整備する

適切な情報管理を行うためには、コンプライアンス(法令遵守)の推進体制を社内に整備しておくことが重要である。情報管理に関してコンプライアンスが求められる法律としては、ソフトウェアの不正コピーの防止などを定めた著作権法や、模倣品・海賊版商品の輸入・販売の禁止などが盛り込まれた不正競争防止法、さらには個人情報保護法、電子署名法、e-文書法などがある。これらの法律については、その趣旨を正確に理解し、遵守に向けた取り組みを実践する必要がある。その実践にあたっては、経営層の中から責

任者を任命して社内に推進組織を設置することが望ましい。なぜなら、コンプライアンスの推進は、自社の経営方針やビジネスプロセスなどと密接に関わるからだ。そのうえで、個々の対策を推進する責任者を任命すれば効果的である。また、自社の情報管理のニーズやプライオリティに応じて必要なリソースを分配し、具体的な施策を計画的に実施する必要がある。

### 情報セキュリティポリシーを策定して定期的に見直す

企業内において効率的な情報管理を実現するためには、情報セキュリティに関するポリシーや関連する諸規程

を定めて、それを確実に実践することが重要である。ポリシーや諸規程を定める際には、他社の実例などのサンプルをそのまま流用し、組織名や役職名などを単純に置き換えるだけでは、自社に合った効果的な情報管理を行うことは難しい。なぜなら、情報管理のあるべき姿は、企業ごとにそれぞれ異なるからだ。従って、自社の実情に合ったポリシーや規程類を策定するためには、社内で十分な討議を行い、自社の組織や業務との整合性を図る必要がある。また、社長をはじめとする経営陣がポリシーの策定に関与し、自ら責任を持つことが肝要である。そうしなければ、ポリシーを実践するために必要な予算や人材などのリソースを投入することが難しくなるからだ。また、ポリシーや諸規程は、情報管理に関する法改正などに対応するため、定期的に見直すことも必要となる。一度策定すれば終わりではないのだ。

### 情報管理の責任者を決めて不正なアクセスを監視する

責任者とポリシーを定めたなら、具体的な管理策だ。現在、適切な管理が行われていない書類や記録媒体から個人情報や漏えいする事故が数多く発生している。個人情報などの重要書類については、記録媒体の管理方法を明確にして厳正な管理を行う必要がある。個人情報保護法では、情報の取得、利用時の手続きや本人からの開示要求への対応など、企業の遵守すべき

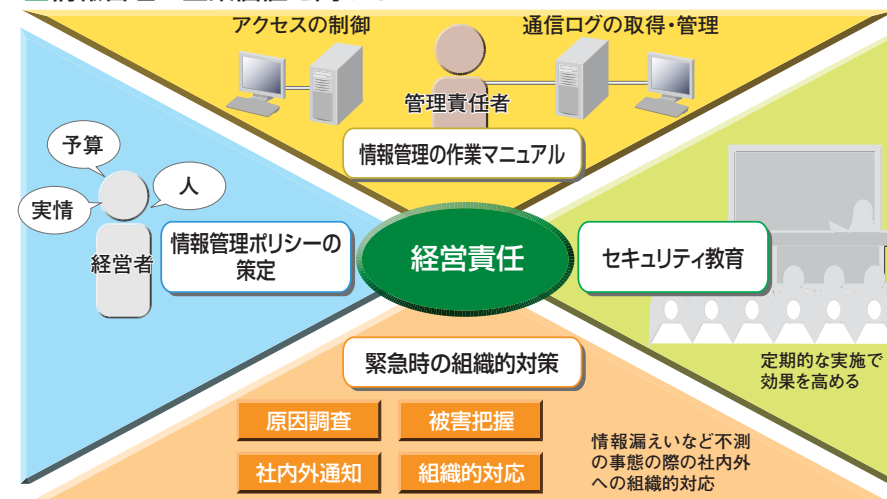
事項が多岐に渡る。このため各工程の作業手順を明確に定め、それらが適切に実施されているかどうかをチェックする責任者を設置することが望ましい。さらに、各工程の作業は決められた担当者だけが実施できるようにしておく必要がある。具体的には、情報が保管されているシステムや書庫にアクセスできる人を制限したり、アクセスできる情報を作業担当者ごとに制限したりすることが求められる。また、作業担当者にはそれぞれIDを付与し、誰が作業を実施したのかわかるようにしておくことが望ましい。そして、重要情報に対するアクセスの記録を定期的にチェックし、不正なアクセスが行われていないか、あるいは、権限外の作業が行われていないか確認することが有効な管理策となる。

さらに、事務所内の机上、書庫、会議室など、身近な場所の整理整頓を行い、重要な情報が記録されている書類や記録媒体が他に紛れ込まないように注意する。その他、郵便物受けの施錠管理、FAX着信物の早期回収、プリントアウトした印刷物の早期回収なども、社内に徹底することが望ましい。また、書類や記録媒体の廃棄処理が不適切であることが原因で情報漏えいする事故も数多く起こっているため、書類や記録媒体はシュレッターなどを使って粉碎処理することも忘れてはならない。

### 情報セキュリティ対策は従業員への教育が不可欠

情報管理の方針が決められたなら、実際に企業内で情報管理を実行するわけだが、その前に従業員に対する情報セキュリティに関する取り組みやルールについて計画的な教育を行い、周知徹底を図ることが肝心である。派遣

### 情報管理で企業価値を高める



社員やパート社員、アルバイトを含めた従業員に対する教育は、ポリシーや関連規程の周知といった全体方針的なものから、パスワードの管理や電子メールを使用する際の注意点といった実務上の項目まで幅広く実施する必要がある。また、入社時の研修などでウイルス対策やOSのパッチ(脆弱性修正プログラム)を適切に実施することや、電子メールを使用する際の注意点、パスワードを扱う際の遵守事項、個人所有のPCの使用規定などを周知徹底させることも重要である。さらに、教育や研修は、すべての従業員に共通のもの、管理職向けなどに分けて実施すると効果的である。最近では、PC上で好きな時間にマイペースで学習できるeラーニングを利用する企業も増えている。集合教育のように従業員を一カ所に集める必要がないので時間と経費を節約できるからだ。

ただし、教育は一度実施しただけで100%の効果が得られるものではないので、法改正などの社会状況の変化に応じながら定期的の実施したほうが良い。また、すべての従業員の教育効果を一定のレベル以上にするために、効果を確認するためのテストを実施したり、何らかのインセンティブを設けたりするなどの施策も必要だろう。

### 万一の事件や事故に備えて事前に対策方法を準備する

そして万一、個人情報漏えいなどの情報セキュリティに関連する事件や事故が発生した場合の対策を事前に準備しておくことも大切である。被害の拡大を防ぎ、被害を限定的なものにするためには、組織全体として事件や事故に必要な対応を適切かつ迅速に行わなければならない。特に個人情報漏えい事件では、事後の対応が遅れると企業イメージが極端に悪くなり、社会的な信用を大きく失墜させてしまうことになる。そうならないためには、事件や事故の形態ごとに実施すべき作業内容を明確にするとともに、現場の社員がいざというときに対応作業を円滑に実行できる体制を整えておくことが大切だ。

具体的には、社内の関係者への報告、システムや業務の一時停止などの緊急処置の実行手順、被害状況や原因の調査と対策の実施、被害者への連絡や社外への周知、業務の再開手順などを明確にしておくこととよいだろう。また、事件や事故の処理には、組織的な対応が不可欠であるため、緊急連絡網を準備しておくことも大切である。

### 情報管理のためのベンチマーク チェックシート 1

(「企業における情報セキュリティガバナンスのあり方に対する研究会 報告書」経済産業省)をもとに編集部で作成

#### 【運用・管理的要素】

- 情報管理ポリシーは、作成済みである。
- 個人情報の取り扱い規定を定めている
- コンプライアンスの推進方法を整えている。
- ISMS (ISO27000)、プライバシーマークなどを取得済み、または取得予定である
- 個人情報などの重要書類、記録媒体の管理(保管や持出し許可、廃棄)方法を明確にしている
- システム上の物理的なセキュリティ状況を把握できている
- 情報管理ポリシーを、定期的に検証している
- 個人情報、重要情報が漏えいした場合の対策を図っている

#### 【人的要素】

- 従業員に自社のセキュリティの取り組みやルールについて継続的、計画的に教育を行い浸透を図っている
- 社内の情報管理の責任者は明確になっている
- 感染Winnyソフトの危険性ととも、個人所有のPCに対して使用規定が周知徹底されている。

## システム化で効率的な情報管理を実現しよう！

実際に情報管理の施策を展開するためには、ICカードを利用した入退室管理やウイルス対策ソフトの導入など、ITを有効活用することが望まれる。それによって、情報管理を効率的に行うことが可能になるからだ。情報管理ベンチマークの「システムの要素」をチェックしたうえで、以下のポイントを参考にしながら情報管理のIT化を推進していきたい。

### ICカードなどを利用した入退室管理で情報を守る

重要な情報や設備がある場所は、セキュリティ対策として、入室可能な人をできるだけ制限したり、外部からの侵入者に対する防護策を強化するなど特段の配慮が必要となる。具体的な対策としては、ICカードや個人認証などを利用した入退館・入退室管理や、赤外線や振動センサーなど防犯用の各種警報設備の設置などが挙げられる。防犯設備などによる侵入対策に加え、セキュリティ境界内に入った人物が許可された人物であるかどうかを一目で確認することも重要だ。よく利用される対策としては、従業員とゲストを名札の色で識別する方法がある。さらに、記録を取ることは犯罪や不正行為の抑止につながる。そのためには、IC

カードによる個人識別などを利用して、入退室時の記録管理を徹底するといった取り組みが必要となる。特に基幹業務システムや機密情報を保有しているシステムは、一般の従業員や来訪者から隔離し、容易に触れない場所に設置することが重要だ。廊下や打ち合わせ場所などのパブリックエリアからは確実に隔離する必要がある。

### ウイルス対策ソフトはアップデートを怠らない

ウイルスやスパイウェア対策としては、インターネットと社内ネットワークの接続点におけるゲートウェイ型ウイルス対策ソフトの導入や、クライアントPC、サーバへのファイル監視型ウイルス対策ソフトの導入が基本となる。しかし、ウイルス対

策ソフトは、一度導入すれば安全だというわけではない。新種のウイルスに対抗するためには、常に最新のパターンファイルをアップデートしておかなければならない。そのためには、パターンファイルの更新や情報収集を行うための全社的な体制を構築しておく必要がある。具体的には、インベントリ管理ソフトウェアなどを利用して、全社のPCが最新のパターンファイルにアップデートされているかどうか確認する。さらに、社内で使用しているOSやソフトウェアについては、セキュリティを考慮した設定や、パッチの適用といった脆弱性対策も重要となる。

また、一般に市販されているウイルス対策ソフトは、新種のウイルスへの対応において完全にウイルスを検出、遮断できるとは限らない。そのため、ウイルスやワームに感染した場合に被害を最小範囲に留めるためには、発見から対応までの迅速な行動が求められる。発見時にはネットワークケーブルを抜くといった物理的な行動に加えて、必要な対策を関係者に指示する手順を明確にしておく必要がある。社内に情報システム担当者を抱える余裕がない場合は、アウトソーシングによる監視サービスなどを導入するとよいだろう。

### 重要情報のやりとりは暗号化して行うのが鉄則

インターネットを利用して本支店

間で通信したり、出張先のホテルなどから社内ネットワークにアクセスしたりする場合は、VPNを導入して経路を暗号化する必要がある。また、重要なメールのやりとりについては、添付書類を暗号化したり、メッセージそのものを暗号化したりすることも必要になる。多くの圧縮ソフトウェアは、ファイルの暗号化機能もサポートしているため、それらを活用するのほひとつの方法である。さらに、社内のネットワークにおいても、重要な通信は暗号化するべきである。たとえば、各部門の経理担当者が経理サーバにアクセスする場合、担当者から経理サーバまでのネットワーク経路が他の部門をまたぐことになる。このような場合、経路の途中で多くの従業員に情報にアクセスする機会をつくってしまう。こうした環

境では、たとえ社内LANであってもVPNを導入して経路を暗号化する、スイッチングハブなどを利用して部門ごとにネットワークを分離することが望ましい。特に無線LANを使用している場合は、建物の外からでも傍受できることがあるため、暗号化通信の設定を必ず行うべきだ。

### ユーザー認証を行ってアクセス制限を実施する

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必要がある。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

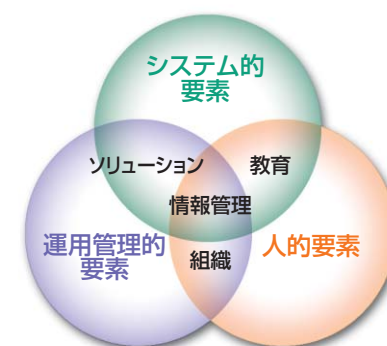
クセス制限を設ける。同じ業務アプリケーションの中でも、閲覧だけ許可する人やデータ変更まで許可する人など、権限区分を設定してアクセス制御を行うことも重要である。また、従業員の異動や退社によってIDが不要になった場合は、そのIDを使って不正にアクセスされないように速やかに削除しなければならない。一方、パスワードについては、誕生日など第三者に推測されやすいものは避けた方がよい。数字や文字だけでなく、記号などを織り交ぜたパスワードを設定するなどの工夫が必要だ。

このようにシステムや機器の導入によって効率的に情報管理を進めると同時に、従業員へのセキュリティを重視する教育、および情報管理を組織的に統括する責任者をはっきりしておくことである。

### 3つの要素のバランスが情報管理を確かなものにする

#### ■情報管理の3要素

情報管理のベンチマークチェックシートの内容は「運用管理」「システム」「人」の3つの要素に分かれている。各要素が重なり合っている部分を確実に実行することで、情報管理が実現できる。



万全な情報管理を実現するために必要となるシステムの要素は、データベースなどへのアクセスログの取得や、災害対策としてのデータバックアップなど、他にもいろいろある。

しかし、情報管理において重要なことは、単にシステムを導入すれば完了するわけではないということだ。まず、経営者が自ら責任を持ってコンプライアンスを推進する体制を社内に整備し、その指針となる情報セキュリティポリシーを策定し、情報管理における運用管理の仕組みを整えておく必要がある。しかし、それを実際に実行していくのは、従業員一人ひとりである。したがって、情報管理における人的要素としての従業員教育を計画的に実施し、情報セキュリティポリシーを具体化する施策を現場レベルで着実に実行していく必要がある。しかし、人手による取り組みには限界があるので、投資対効果を考慮したうえで、ITを積極的に活

用したい。すなわち、情報管理におけるシステムの要素を上手に活用しながら、情報管理を効率的に推進することが重要なポイントになる。

このように、企業が適切な情報管理を行うためには、「運用管理的要素」、「人的要素」、そして「システムの要素」をバランスよくとりながら、具体的な個々の施策を着実に実施していくことが求められる。逆に言えば、「運用管理的要素」「人的要素」「システムの要素」のどれかが欠如していると、コンプライアンスを実現する最適な情報管理を行うために時間がかかったり、困難になったりすることになる。

今回の、情報管理ベンチマークを通じて自社の情報管理の現状を認識し、どの要素に脆弱性があるかを判断して、それを補うための取り組みを実施していきたい。そうすることで、IT社会における社会的信頼と評価を高めることができるのだ。

### ○ 情報管理のためのベンチマーク チェックシート 2

#### 【システムの要素】

- セキュリティの重要度が高い部屋には、セキュリティ対策が施されている
- セキュリティ対策としてワーム、スパイウェアなどの不正対策ソフトを導入している
- セキュリティを考慮した設定や、パッチの適用といった修正プログラム、脆弱性対策を実施している
- ネットワークデータに暗号化などの保護策をとっている
- 情報データへのアクセス制限、認証手段を採用している

# 何でも相談、24時間対応、最新メディアを配送 Red Hat Enterprise Linux『Plus』シリーズの新サポート

テンアートニが提供しているスペシャルサポートサービスRed Hat Enterprise Linux『Plus』シリーズに、また新たなサービスが付加された。いずれも、かゆいところに手が届く、お客様の視点に立った便利なサービスである。是非、有効活用していただきたい。

## ■ハードベンダー5社と連携し、障害切り分けサービスを開始

『Red Hat Enterprise Linux』は、エンタープライズに適したLinux OSとして圧倒的なシェアを誇っている。テンアートニでは、きめ細かなサポートサービスを提供してほしいというニーズに応え、さまざまなサービスを付加したスペシャルサポートサービスRed Hat Enterprise Linux『Plus』シリーズ(以下『Plus』シリーズ)を提供している。今回、その中で新たな付加サービスとして、障害発生時の問い合わせ先を一本化する、ハードウェア/ソフトウェア切り分け支援サービスを3月30日から提供開始した。

これまで『Plus』シリーズでは、サポート範囲がOSのみだったが、何か障害が発生した場合に、その原因がOSなのか、ドライバーなのか、あるいは、ハードウェアなのかお客様側で判断することが難しいケースがある。そのため、お客様から障害時の問い合わせ窓口を簡素化してほしいという要望が数多くあった。今回の新サポートはその要望に応えたもので、障害の原因がどこにあるのかわからない場合でも、テンアートニが一括して問い合わせを受け付ける。そして、OS以外に起因する問題の場合は、その製品を提供するハードウェアベンダーへハードウェア障害であるかどうかの確認作業を、テンアートニが代行する。そ

の調査の結果、ハードウェアに起因と判断した時点で、ハードウェアメーカーのサポート部門と連携して問題点を把握し、解決方法を提案する。これにより、障害時の迅速な復旧を実現するのだ。しかも、『Plus』シリーズのユーザーであれば、別途料金はかからない。

この新サービスが可能になったのは、主要なハードウェアベンダーである日本アイ・ビー・エム、NEC、日本HP、日立製作所、富士通の5社とテンアートニがバックエンドサポート契約を結び、各社と連携を図りながらハードウェアを含めた解決方法をお客様に提供できるようになったからだ。そのサポート対象ハードウェアは、日本アイ・ビー・エムのIBM xSeriesとIBM BladeCenter、NECのExpress5800シリーズ、日本ヒューレット・パッカートのHP ProLiant サーバ、日立製作所のHA8000シリーズ、富士通のPRIMERGYである。

## ■『Premium Plus』によって24時間いつでもサポート!

『Standard Plus』のサポートは、朝9時から夜21時まで電話による問い合わせに対応するテクニカルサポートを提供している。これは、現場で対応する技術者の要望に

応えたものだ。このサポートでは、新規・再インストール時やErrataやアップデートに起因する問題が発生したときなどにテクニカルサポートを受けることができる。しかし、『Red Hat Enterprise Linux』が、ミッションクリティカルなエンタープライズ用途に利用されるようになり、24時間365日止まらないシステムを構築することが当たり前前の時代となった。そのため、夜21時以降のテクニカルサポートも提供してほしいという要望が出てきた。

そこで、テンアートニでは『Plus』シリーズに『Premium Plus』を加えた。『Premium Plus』とは、夜21時から朝9時までの時間帯で、専用サポートオペレータが待機し、サーバトラブルによるシステムダウンなどの重大な障害(重大性レベル1:お客様の生産システムの停止、重大な影響を与えるような問題やシステム上のデータが失われ、解決方法が行われていない状態。重大なセキュリティ侵害を引き起こす可能性がある状況)に対応するサポートである。電話問い合わせの際、テンアートニ側で蓄積してきたノウハウをもとに、新たな調査を行わなくても済む内容については、原則的に1時間以内で回答する。これにより、お客様は9時から21時までの日中のサポートとともに、24時間体制のサポートシステムにより、安心して『Red Hat Enterprise Linux』を運用することが可能になる。

『Red Hat Enterprise Linux』は、『AS』と『ES』、『WS』の3種類あるが、この『Premium Plus』のサポートは、『AS』と『ES』の2種類を対象にしている。

ちなみに、レッドハット社にもPremiumサポートサービスがあり、『AS』のみを対象としている。朝9時から夕方17時までが日中のサポート対応で、17時から朝9時までが重大障害のみの夜間対応となる。一方、テンアートニの『Premium Plus』は、朝9時から夜21時まで日中のサポートを行うので、4時間分厚いサポートが受けられる。

## ■アップデートメディアを配送 国内初の新サービスを提供

さらにテンアートニでは、3つ目の新サービスとして、「アップデートメディア・デリバリーサービス」を開始した。同サービスは、『Plus』シリーズの新規購入時にWeb上でユーザー登録する際に、最新版のOSのメディアがほしいと申し込めば、最新版のメディアをソース込みでフルセットで提供するもの。もちろん、メディア代や送料などは一切かからない。

レッドハット社では基本的なポリシーとして、出荷時に初期版のメディアを配送している。例えば最新機種ハードウェアでは、ドライバーなどの関係でアップデート3以上のものでないとインストールできないものもある。その場合、ユーザーは、自分自身でアップデート3以上のものをダウンロードしてインストールしなければならない。

こうしたことからレッドハット社の最新版のOSは、ユーザー自身がRed Hat Networkにアクセスしてダウンロードしなければならない。しかし、最新版のOSはかなりのボリュームになるため、ダウンロードするだけで数時間かかり、それをメディアに取り込んでハードウェアにインストールするまで相当の手間と時間がかかる。そのため、初期導入時くらいは最新版のOSが入ったメディアを提供してほしいという要望が数多くあった。

そこで、テンアートニでは、そうした問題を解消するためにお客様に対するサービス優先の視点に立った国内初のサポートサービスとして今回提供するに至った。現在は『ES』のみの対応だが、今後、ニーズがあれば『AS』などにも対応していく考えだ。

今回紹介した『Plus』シリーズは、大塚商会 BP事業部経由で購入できるので、パートナーの皆様は、他社との差別化を図る商材として是非有効活用していただきたい。

### ●Red Hat Enterprise Linux『Plus』シリーズ

Red Hat Enterprise Linux AS	大規模なネットワークシステムやデータベースERP、CRMサーバなどを含むデータセンターなどのハイエンド・サーバソリューション。
Red Hat Enterprise Linux ES	ファイルサーバ、メールサーバ、Webサーバなどの幅広いネットワークシステムでのご利用に最適なサーバソリューション。
Red Hat Enterprise Linux WS	Linuxのパワーユーザー向けの、ビジュアライゼーション、ソフト開発、及びエンジニアリングデザイン等の幅広い、ハイパフォーマンスなアプリケーションに最適。

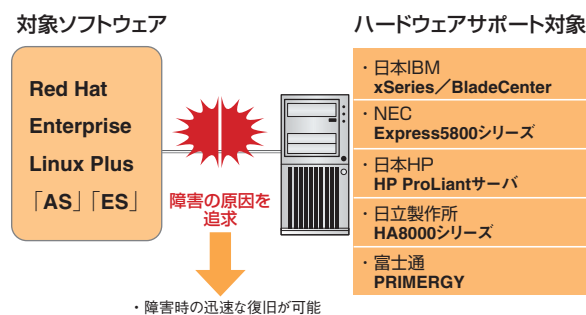
### Red Hat Enterprise Linux『Standard Plus』のサービス&サポート

- 専任技術者による9時から21時までのテクニカルサポート
- サブスクリプション(購読権)は、更新1年目から10%の割引で提供、3年間での更新はさらに割安な定価設定
- 1年、3年、5年の複数年契約は、単年度契約よりも安く、わずらわしい更新手続きも不要
- SELinuxを導入者自身で有効的に導入・運用ができるよう支援する「システム構築サービス」「運用サポートサービス」のメニューを用意

### Red Hat Enterprise Linux『Plus』シリーズ

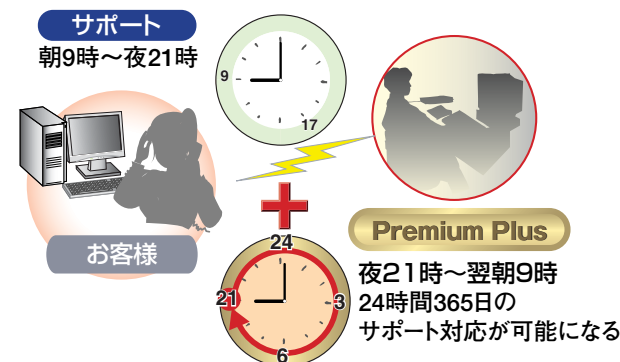
#### ●新サポート1 困った時は 障害切り分け支援サービス

システム障害で、原因がわかりにくい時は、とにかく問い合わせ。テンアートニで障害の原因の切り分けを支援 ※平日9時から21時までのサービスとなる



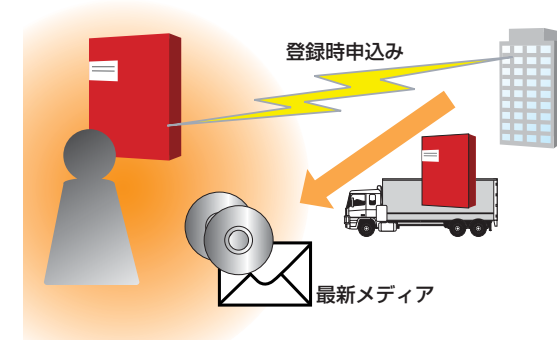
#### ●新サポート2 いつでも応答 『Premium Plus』

『Premium Plus』なら朝9時から夜21時までの日中のサポートに加え、夜21時から翌朝9時までの対応で24時間サポート ※このサポート対象は『AS』『ES』のみ ※『Standard Plus』とは価格体系が異なる



#### ●新サポート3 アップデートメディアデリバリーサービス

初期導入時のユーザー登録時に最新メディアを申し込めば、メディア代、配送費無償で届けられるので、最新版をダウンロードする手間や時間が省ける ※サポート対象は現在『ES』のみ





## 業務改革・改善のための

## IT活用とは

第7回

## セキュリティとコンプライアンスに向けた取り組みの第一歩とは

業務改革・改善のためには、どのようなIT活用の方法があるのだろうか。パッケージ化されたアプリケーションの利用によって、どこまで効率は上げられるのか。あるいは、ビジネス系アプリケーションの使いこなしによって改善が図れるのか。そうした視点から、IT活用について考えていく。今回はセキュリティとコンプライアンスについて考察する。

## 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、産業界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。2004年以降、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。

セキュリティの最も基本となる  
統合ID認証とは

個人情報保護法の施行に合わせて、社内に散在する個人情報を一か所に統合したり、利用者制限を設けて安全性を確保するため、何かしらの対策を実施している会社は多いのではないだろうか。セキュリティの基本は、「制限」にある。これまでのIT活用の基本は、必要な情報をいつでも誰でも簡単に手に入れられることであった。しかし、セキュリティという観点になると、それは反対になる。きちんと管理された情報が、あらかじめ承認された人だけに、必要最低限に届けられることが、もっとも重要な仕組みとなる。そのために、ITでできることの第一歩が、統合ID認証の確立である。

この統合ID認証とは、シングルサインオン(SSO)と呼ばれることも多い。つまり、社内のネットワークにひとつのユーザー名とパスワードでログインして、すべての利用権が統合的に安全に管理されている状態を目指すものだ。いたってシンプルな目的だが、これを実現している企業は少ない。たとえば、

社内のネットワークにはWindowsのActive Directoryによるログイン処理を行っているのに、社内ポータルでは別のユーザーIDを入力し、さらにグループウェアでも違うIDが必要になる、というケースは多いのではないだろうか。さらに、業務用アプリケーションごとにユーザーIDが違う例も多い。

こうしたIDの乱立が起きてしまう背景には、アプリケーションを導入した時期の違いや、ネットワークを構築したときのアーキテクチャの違いがある。多くの企業では、段階的にシステムを導入してきたために、構築した時点のオープンシステムに合わせて、ログインIDやユーザー名の管理が、まったくバラバラになっているのだ。もちろん、こうした会社の情報システムでは、ユーザーIDに関する統一化されたポリシーもなければ、しっかりとした管理も行われていない。

記憶に新しい某大手通信系企業の情報漏えい事件でも、退職した社員のユーザーIDが残っていたために、不正にアクセスされて顧客情報が流出してしまったのだ。こうした事件を起こさ

ないためには、退職と同時にユーザーIDが迅速に削除される社内体制を整備することはもとより、IDそのものの管理が一元化されていなければならない。そのためには、全社規模で統合化できるID認証基盤技術を導入する必要がある。

コンプライアンスに欠かせない  
業務処理の透明化とID認証の重要性

一方、日本版SOX法に向けた対策のひとつに、企業としての説明責任や承認プロセスの明確化といったテーマがある。不正経理や利益操作ができないようにするためには、日々の業務処理において適正な承認プロセスが行われているか、経理担当者が単独決済ではなく、複数承認によるチェック機構を維持しているかなど、業務の流れを改めて見直す必要が出てきている。こうした課題に対して、いまITソリューションとして注目されているのが、先月も紹介したワークフローシステムである。

ワークフローシステムの基本は、電

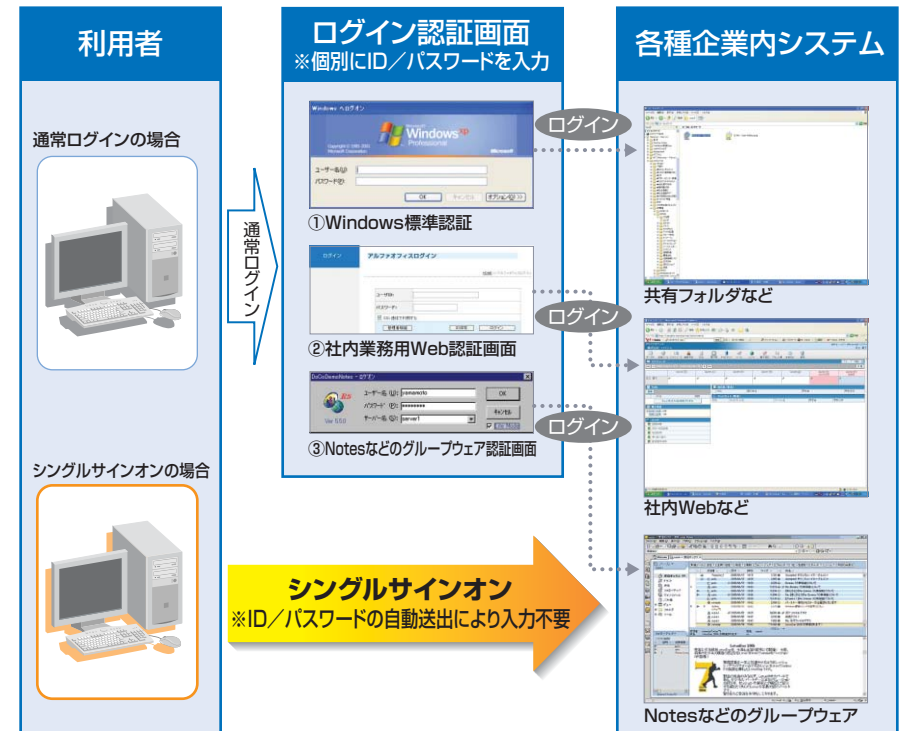
子承認プロセスの実現にある。これまで、紙で回覧していた稟議書や申請書に伝票などの書類を電子化し、それを設定した承認者に対してネットワークで回覧し、承認を得て行く仕組みである。いわば、電子伝票処理だ。ワークフローによる電子伝票処理の効果は、二週間以上かかっていた承認時間が、半分から二日という短時間になるということだ。その効果に加えて、いま注目されているのが、コンプライアンスに貢献するプロセスの透明化と説明責任の実現である。

ワークフローがない会社では、ひとつの売上や請求処理に対して、そのすべてを紙に書いて明確化する必要がある。売上だけではなく、購買や借入れなど、決済に関わるすべての業務を透明化し、その説明を明確にしていかなければ、企業としてのコンプライアンスは確立できない。それを手作業で行うことは、現在の企業活動において不可能とはいえないものの、膨大な手間と時間とコストがかかることは事実だ。それをさらに、定期的に監査しながら報告書も作成することを継続していくと考えると、IT化しなければ合理化も省コスト化もできないのだ。こうした観点から、ワークフローシステムの導入を検討するケースも出てきている。

ワークフローの実現においても  
重要になるシングルサインオン

ワークフローを導入するにあたって、どのような製品を選ぶかは、実際の作業において重要なポイントとなるが、それに加えて重要なテーマが、先に解説したシングルサインオンの確立になる。ワークフローシステムでは、印鑑の代わりにログインしている個人のユーザーIDが、すべての基本になる。つまり、誰かが不正にログ

## ●統合ID認証(シングルサインオン)



●シングルサインオンなら一度認証を受けるだけで、LANへの接続、社内Webなどのすべての機能が利用できる

インして承認してしまえば、コンプライアンスの根幹が崩れることになる。反対に、適正なユーザーIDの管理が行われていれば、代理承認や承認フローの修正なども、きちんと記録され監査証跡として残すことができる。このような目的において、すべての基本がユーザーIDの正当性と健全性になってくる。

さらに安全性を高めるのであれば、社員ICカードや指紋認証などと組み合わせ、PCの利用そのものをガードすることが、必要になるケースもある。もちろん、あまりにもセキュリティを固めすぎて、利用者の利便性を欠いてしまえば、IT本来の利活用を促進できなくなる心配はある。しかし、これまでのオープン化一辺倒だったシステム構築の方向性から、管理と監視を前提としたシステム基盤を考える必要が出てきている。シングルサインオ

ンは、理屈としては簡単な仕組みであるが、それを実際に全社規模で導入するには、IT部門だけの努力では実現されない。

人事や総務に危機管理室など、人を司る部門との連携をとって、足並みを揃えた導入への取り組みが求められる。加えて、社員教育も重要だ。単にIDカードやログイン認証で縛るのではなく、企業構成員としてどうあるべきか、セキュリティとコンプライアンスに対する意識や必要性を教育し啓蒙していく活動も求められる。

こうした状況になってきたのも、ITがこれまでのような「便利な文房具」という役割を越えて、企業活動そのものに不可欠なインフラとしての責任を担っているからだ。それだけに、企業の中でITに関わる人たちにも、これまで以上の意識や取り組みが求められているのだ。

# 売れるショップに売れる人

第7回

## 現代に通じる近江商人の心意気

島川 言成 氏

先日、名古屋に本社を構える企業の経営者とお話しする機会を持ちました。東京・大阪よりも景気が先行して良くなった名古屋ですが、「何が原因なんだろうね？」と質問したところ、「近江商人の血が濃い場所だから…」と教えられました。「近江の千両天秤」という諺がありますが、天秤棒一本あれば行商で千両を稼ぎ、財産を形成するのが近江商人の真骨頂であり、千両を稼いでも行商を続ける「継続は美」というDNAも有名です。

「IT時代に近江商人とは」と呆れる人もいるでしょうが、果たしてそうでしょうか？歩いて販路を広げることは、非常にリアルなビジネスです。近江商人が得意としたのは、商品に関する需要と供給の状況、地域による価格差などを商業活動に活用したことでした。リアルなビジネスで一定の販路を獲得すると、蓄財した資本で、全国各地に積極的に支店を開設したことも近江商人の特長です。支店展開で成功すると、江戸の日本橋、大阪の本町、京都の室町という三都にも進出する豪商に成長したのが近江商人でした。

近江商人のビジネスモデルに「産物廻し」があります。持ち下り荷(関西から関東や地方へ)・登せ荷(地方から関西や江戸へ)など、地域間の需給と価格差に着目して生産地から消費地へ生活必需品を流通させるのです。IT時代の現在は商圏がワールドワイドに拡大しただけで、実態は近江商人の行為と変わりがありません。多くの近江商人は金融業・質屋なども経営していました。貸したお金の返済は、金銭だけでなく、大豆などの現物で返させてもいました。大豆は醸造業に関係深い原材料ですが、実際にそれに進出した近江商人もいましたし、明治以降、多くの商人が銀行を設立しました。

近江商人は、地方へ資本と技術を提供して、原料を移入し製品を移出するというビジネスモデルも作っています。また、紅、酒、油などの製造権も取得して、原料を仕入れ、技術者を雇って製造販売した近江商人もいました。近江商人たちは、経営の範囲が広がると個人企業から何人かが資本を出し合い、共同企業(乗合商合)を組織したそうです。近代資本主義経済の先取りですね。組織は商人たちが自己の商権を守り、相互の不要な競争をさける目的もありました。

成功した近江商人の家訓は貴重です。共通することは、勤勉・倅約・正直・堅実・寛容です。代表的な家訓に「しまつて、きばる」があります。どういう意味でしょうか？近江商人の商法は、八幡商人・日野商人・五個荘商人など、活躍した時代や場

所により異なりますが、共通するのは遠い地域間の価格差を利用すること、商売相手の利益を優先するという考えです。つまり、薄利の商売だったので、利益を上げるために、他人の嫌がる苦勞を進んで「きばり」、長期的にみて経済の合理性を求めることが「しまつ」です。近江商人にはケチという印象

を持つ人がいますが「しまつ」を誤解されたものなのです。「三方よし(さんぼうよし)」という五個荘商人中村治兵衛の家訓があります。「他国へ行商するもの総て我事のみと思はず、其の国一切の人を大切に、私利を貪ること勿れ…」ということです。「売手よし」「買手よし」だけでなく「世間よし」を考慮せよとは、まさに現代の企業に求められている姿そのものだと思いますか？

「富を好しとし、其の徳を施せ」は、八幡商人西川利右衛門の家訓でした。商売が繁盛して富を得るのは良い事だが、その財産に見合った徳(社会的貢献)をすることも重要だと教えます。業績が大きくなった分だけ、企業の社会的貢献という徳を積みなさいということです。このことから、近江商人の現代性が認められます。名古屋の経営者は「名古屋人はケチと話す人がいるけど、冗談じゃない、使うべきところには使うという信念が強いだけ」と話します。「ケチ」と誤解されながらも、近江商人の「しまつ」の商いに自負を持っているのです。

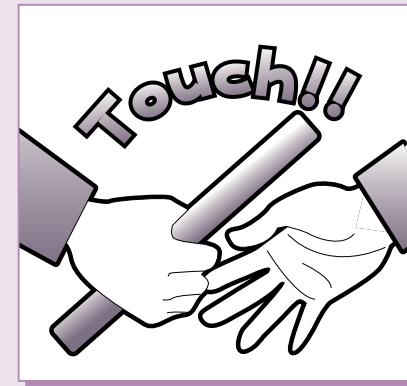
### 島川 言成

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」創作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、ゲームクリエイ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

### 大手電機メーカーの相次ぐ社長交代、その共通項とは？



第7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)、月刊アスキー(アスキー)などで連載および定期記事を執筆中。著書に、「ソニースピリットはよみがえるか」(日経BP社刊)、「松下電器変革への挑戦」(宝島社刊)など。

営理念に基づく経営」という点だ。日立製作所の新社長に就任した古川 一夫氏は、「社長就任までの間、社史を紐解き、日立創業の地を訪れました。創業者である小平浪平が国産技術の振興を目指したときの創業の理念を改めて思い起こしました」と自らの経営のベースに創業時の理念を持ち込むことを示した。

また、東芝の西田 厚聡社長も「東芝は、創業以来、数多くの優れた技術と、高い品質の商品、サービスを創出するわが国を代表する電機メーカーに成長しました。2005年に創立130年を迎え、この節目にふさわしい最先端の商品、技術を世に送り出し、東芝というブランドがまた新たな輝きを獲得できるようにしたいです」と語る。

一方、松下電器の新社長に就任する大坪 文雄氏は、「環境変化が大きければ大きいほど見失ってはいけないのが、創業者の経営理念です」と、創業者である松下 幸之助氏の考え方を、経営の根幹に置くことを示して見せた。大坪次期社長は、創業者の理念のなかでも、「衆知を集める」という言葉を好み、自らの経営も「衆知を集めた経営としたい」と語る。

NECの新社長となった矢野 薫社長は、東大卒、通信畑出身の人間である。歴代のNECの社長は通信畑出身の人間であったが、前社長とその前の社長はコンピュータ畑出身であった。2代続いたコンピュータ畑出身の社長体制から、久しぶりにかつてのNECの王道な社長人事に戻ったといえる。矢野社長は就任直後から、「NGN(次世代ネットワーク)」といったネットワーク関連のキーワードを連発しているため、NECの原点ともいえるネットワーク事業を成長エンジンとした事業形態へと回帰して

いることを感じさせる。

もうひとつの共通点として、大手電機メーカー新社長に共通的に課せられたのがグローバル戦略だろう。何故なら、海外事業比率の引き上げとともに、海外における成功がそのまま全社成長戦略につながるからだ。

新社長に海外での事業経験者が多いこともそれを強く感じさせる。ウェールズ生まれの米国人であるソニーのハワード・ストリンガーCEOは、米国でソニーを立て直した実績はもとより、強いブランド力を誇る北米市場を足がかりに復活の道を模索するには最適な人物だといえる。松下電器の大坪次期社長、NECの矢野社長も、海外現地法人での社長経験者だ。また、東芝の西田社長も、東芝の海外法人から入社したという異例ともいえる経歴の持ち主である。いずれも海外での深い経験が、新社長の舵取りに活かされることになりそうだ。

実際、新社長からもグローバルを意識する言葉が相次いで聞かれている。「2010年には、グローバルエクセレントカンパニーを目指す」というのは松下電器の大坪次期社長の言葉で、「世界のエクセレントカンパニーとして輝くことを目標とする」というのは日立製作所の古川社長の言葉である。これらのグローバル展開を前提とした取り組みが各社の成長戦略の鍵となりそうだ。

このように各社の置かれた立場は異なるものの、日本のものづくりの根幹ともいえる大手電機メーカー各社の創業時の理念を経営に生かすこと、そして、それをベースとしたグローバル戦略を展開していくことは各社に共通したものだといえる。

新社長体制となった大手電機メーカー各社の新社長たちの手腕がどう発揮されるのか注目したい。

第19回 アドビシステムズ株式会社

# アドビ製品を自由に組み合わせて購入できる 新ライセンスプログラム『Adobe Open Options 4.5』

アドビシステムズ株式会社は、昨年12月にマクロメディア社を買収し、多様性に優れた革新的な製品を数多く保有する世界有数のソフトウェア企業として新たなスタートを切った。これに伴い、今年1月から新ライセンスプログラム『Adobe Open Options 4.5』を導入し、より多くの導入メリットがもたらされるようになっている。そのライセンスメリットについて詳しく紹介する。

## 導入コストや運用管理を軽減する主なメリット

アドビシステムズ株式会社(以下アドビ)の新ライセンスプログラム『Adobe Open Options 4.5』は、アドビ製品のソフトウェアをインストールして使用する権利を販売するもので、今回から一般法人向けや教育機関向けでも1ライセンスからライセンスプログラムのメリットを享受できるようになった。また、旧マクロメディア社の製品にも同じライセンスプログラムが適用される。例えば、これまでマクロメディアの製品は旧バージョンへのダウングレード使用が認められていなかったが、アドビ製品と同様に申請可能となった。取引先と同じバージョン

の製品を揃えてプロジェクトを円滑に進めたい場合などに有効だ。

新ライセンスプログラムの主な特長は下表の点がある。まず、導入する製品のライセンス数に応じてポイントが加算され、その合計数によって価格レベルが決定される。つまり、ライセンスポイントが増えるほど割引率が高くなる。次に、ソフトウェアの運用の手間を軽減できることだ。ひとつのシリアルナンバーと1枚のCD-ROMで複数のPCへインストールすることができるので、ユーザー登録を個別に行う煩雑さが解消される。三つ目は、部材の保管スペースを大幅に削減できることだ。

四つ目に最も大きな特長として、OS環境の変更に柔軟に対応できるこ

とだ。パッケージ製品の場合は購入時にOSが限定されてしまうが、ライセンス製品は、最初からMac版とWindows版の両方のシリアル番号を配布しているので、Mac版からWindows版へ、あるいはWindows版からMac版へライセンス数の範囲内で容易にプラットフォームを移行することができる。

五つ目は、オプションで『アップグレードプラン』を別途購入することにより、契約期間中ならいつでも最新バージョンへアップグレードできること。そして六つ目は、ポイント数の範囲内でアドビ製品を自由に組み合わせてライセンス購入できることである。この発注の柔軟性は、他社のライセンス制度にはないメリットだといえるだろう。

## ◆ライセンスプログラム6つのメリット

- 1 導入するライセンス数が増えるほど割引率がアップ**  
導入されるライセンス数をポイントに換算し、ポイントの合計数によって価格レベルが決定する。なお、ポイント数は製品によって異なるので、右サイトから最新のポイント表で確認が必要。 <http://www.adobe.co.jp/aoo>
- 2 ソフトウェア運用の手間が軽減できる**  
アドビライセンスプログラムでは、ひとつのシリアルナンバーと1枚のCD-ROMで複数のPCにインストール可能なため、ユーザー登録を個別に行う煩雑な作業が軽減でき、ライセンスプログラムを利用してアップグレードすることで、すでに所持しているパッケージ製品のライセンスも一元管理できる
- 3 部材の保管スペースを大幅に削減**  
CD-ROMやユーザーマニュアルは必要な数だけ購入できるので、余分なパッケージやマニュアルを保管・管理する必要がなく、スペースを削減できる
- 4 OS環境を変更して使用することが可能**  
Mac版からWin版へ、あるいはWin版からMac版へライセンス数の範囲以内で容易にプラットフォームを移行することが可能になる
- 5 常に最新バージョンが利用可能**  
『アップグレードプラン』を別途購入すれば、常に最新バージョンのアドビ製品を利用できる
- 6 オーダーの組み合わせは自由**  
本プログラムは、ほとんどのアドビ製品を対象としているため、製品カテゴリーにかかわらず、自由に組み合わせてオーダーできる。新規ライセンスとアップグレードライセンスを組み合わせたり、Win版とMac版を混在して利用することも可能になっている

## ◆企業の導入規模に合わせた2つのライセンスプログラム

『Adobe Open Options 4.5』には、2つのプログラムが用意されている。このうち『Transactional License Program 4.5』(以下TLP)は、日本国内のひとつの一般法人に対して適用されるライセンスプログラムで、導入する製品の種類や数に応じた多彩な組み合わせに対応し、1度の発注時のポイント合計に応じて3段階の価格レベルでディスカウントされる(表1)。1ライセンスから購入でき、購入申込書を提出するだけなので小

規模事務所でも手軽に利用できる。

一方、『Contractual License Program 4.5』(以下CLP)は、お客様とアドビ社が2年間の契約を結ぶことで海外拠点や子会社、関連会社まで含めて適用されるライセンスプログラムであり、4段階の価格レベルでディスカウントされる(表2)。CLPは初回導入時に4万ポイント以上から適用できる。契約期間中に追加オーダーするとその分が累計ポイントに加算され、次の価格レベルのポイントに達すると、翌月からの購入時に新しい価格レベルが適用される点がメリットだ。従って、大量導入や追加導入が見込まれる場合は、CLPを選択した方がTLPよりもメリットが多いといえる。

## ◆教育機関向けや官公庁向けのライセンスプログラムも提供

アドビ製品は、教育機関でも非常にニーズが多い。そのため、教育機関向けライセンスプログラム『Adobe Open Options 4.5 for Education』が用意されている。TLPとCLPの両方に対応しており、TLPは1ポイントから、CLPは6,000ポイントから導入が可能だ。またTLP、CLPの価格レベルのポイント数設定も一般法人向けよりも少なめに設定されていて利用しやすい。ただし、旧マクロメディア製品の教育機関向けライセンスプログラムと『Adobe Open Options 4.5 for Education』では対象機関の定義が異なる場合があるので事前に確認する必要がある。

## ◆自動ポイント計算などによりライセンス管理の手間を削減

実際にアドビ製品をライセンス購入する際には、自社のライセンスポイントが累計でどれだけあり、どの価格レベルで購入できるか確認する必要がある。

ある。その手間を低減するため、エンドユーザーや販売パートナーが、アドビ社のライセンスプログラムページより自動ポイント計算用PDFをダウンロードすることによって、現在の累計ポイントを自動的に計算できる仕組みを提供している。また、いざ『Adobe Open Options 4.5』で製品を購入するにも、ユーザーが既に保有しているライセンスを把握していないこともあるだろう。この場合、過去の購入履歴の確認が必要になる。これはエンドユーザーが直接、アドビライセンスコールセンターに電話で問い合わせることもできるが、大塚商会や販売パートナーを通じて問い合わせることもで

## ◆ポイント数により選べるプラン



表1:TLP価格レベル(企業向けプログラム)

レベル	ポイント数
0	1 ~ 1,499
1	1,500 ~ 24,999
2	25,000 ~ 49,999

表2:CLP価格レベル(企業向けプログラム)

レベル	ポイント数
1	40,000 ~ 99,999
2	100,000 ~ 224,999
3	225,000 ~ 349,999
4	350,000 ~

## ◆TLP4.5・CLP4.5比較表

	TLP 4.5	CLP 4.5
各プログラムが想定している環境		
導入規模	中堅・中小規模の企業から部門、ワークグループ、大企業	大企業およびグローバル企業
概要		
価格レベルの決定	オーダー毎の合計ポイント数で価格レベルを決定	契約時の初回オーダーポイントで価格レベルを決定。契約期間中の購入累計ポイントが次の価格レベルに達していた場合、そのレベルを翌日より適用
使用開始	ライセンス取得後、インストールして使用可能	製品ごとにライセンスを取得後、インストールして使用可能
シリアルナンバー	製品毎、OS毎1つのシリアルナンバーでインストール可能	製品を取得後、その製品のシリアルナンバー(マスターシリアル)を提供
契約の有効期間	-	2年間
アップグレード	最低発注単位以上であれば、保有するライセンス数の一部だけでもアップグレードできる。アップグレードプランを付加することも可能	保有するライセンス数の一部だけでもアップグレードできる。また、過去に購入したライセンスについても、それらが最新バージョンであれば、CLP契約締結後、半年以内なら「アップグレードプラン」の購入が可能
マルチプラットフォームの使用権	可 (Windows版、Macintosh版のみ)	同左
すでに保有しているライセンスの取り扱い	旧バージョン:ライセンス価格にて最新バージョンにアップグレードすることによりポイントに加算可能 最新バージョン:アップグレードプランを付すことで購入ポイントに加算可能	旧バージョン:同左 最新バージョン:一定期間内にアップグレードプランを付すことで購入ポイントに加算可能
ポイントの累計システム	なし	あり。毎月25日にライセンスシステムでポイントレビュー