NRI 未来創発
Dream up the future.

ITソリューション フロンティア
IT Solutions Frontier

特集「文書管理から始める情報資産管理」

05 | 2011 Vol.28 No.5
(通巻329号)

www.nri.co.jp

野村総合研究所
Nomura Research Institute

Adobe Readerのメニューバーで「表示(V)→ページ表示(P)」にある「見開きページ(U)」と「見開きページモードで表紙をレイアウト(V)」の2か所にチェックすると紙面のイメージでご覧頂けます。また、両面プリンターをご使用の場合、印刷時に「ページの拡大/縮小(S)」で「小冊子の印刷」を選択すると紙面に近い状態を再現できます。

ITソリューション フロンティア
IT Solutions Frontier
05／2011

NRI Web Site

IT経営の鍵は“ビジョン×IT活用人材”

経済産業省が2007年に創設した「中小企業IT経営力大賞」という表彰制度がある。優れたIT経営を実現し、かつ他の企業の取り組みの参考となるような中小企業や組織に大賞（経済産業大臣賞）や優秀賞などが贈られる。IT経営とは、ITを新しいビジネスツールとして、業務効率化のほか業務プロセスの再構築や営業・マーケティングの改革などに取り組む経営スタイルとされている。2011年は240件の応募の中から18の企業・個人が表彰された。大賞を受賞したのはワイ・インターナショナル（埼玉県志木市）とグルメン（東京都港区）の２社である。

1898年創業のワイ・インターナショナルはスポーツサイクルの販売を手がけ、首都圏や大阪・名古屋に23店舗を展開している。社長の吉田靖夫氏は、「自転車は地球環境を守る乗り物であり、日本でもスポーツサイクルを欧州並みの文化に育て上げたい」という理念で経営に当たっている。

スポーツサイクルは自転車でも特殊な分野で、顧客層を広げることに加えて顧客ごとの個別ニーズにきちんと対応することが重要だという。そのため同社の各店舗はそれぞれの商圏と顧客層に応じた独自のコンセプトで店づくりがされており、インターネットでの情報提供も店舗ごとに工夫が凝らされている。５万アイテムの在庫管理のほか、自転車をカスタムメードする際に顧客の体型に合わせてシミュレーションするシステムなどがIT化されている。

1984年創業のグルメンは、食品スーパー事業のほか、中小スーパー向けの加工食品の共同配送を行っている。首都圏に８カ所の物流センターと、450台のトラックを保有するという。社長の澤田幸雄氏は流通の無駄をなくす“流通カイゼン屋”を自任し、物流・卸・小売の連携事業による中小店舗の活性化を目指して経営に当たっている。

過剰生産になってしまった大手小売向けの加工食品を安く仕入れて中小小売に廉価に供給する事業も拡大している。当初はファックスで情報交換していたが現在では会員制の取引サイト「なび市－net」を開設している。このほか、物流センターの一連の業務（入荷、在庫からの取り出し、出荷など）の総合管理、ICタグによるトレーサビリティのシステムなどがIT化されている。

大賞を受賞した２社はいずれも社長が明確な経営姿勢と熱意を持って経営に当たっている。これによって芯の通ったIT活用が実現されている。社長自身がITに精通しているわけではないというが、社内・社外の人材を活用して体制を作りIT経営を実践できることを証明している。これは企業の規模を問わないだろう。

激変する昨今の経営環境下では、経営戦略の重要性が特に高いことは言うまでもない。

野村総合研究所
理事
稲月　修（いなつきおさむ）

経営戦略を推進する上で、ITの活用は、業務の効率化・省力化だけでなく戦略推進の基盤となっている。そのIT活用に当たって、多くの企業ではCIO（最高情報責任者）を置いてIT戦略の責任者としている。CIOは経営トップとIT部門の間で、両者の相互理解を深めつつIT戦略を推進する役目を持つ。

野村総合研究所（以下、NRI）では「ユーザ企業のIT活用実態調査」を毎年実施しており、その中でCIOの経歴を聞いている。最新の調査では、IT部門出身のCIOは20％にすぎず、残りは経営企画部門出身（25％）、現場ライン部門出身（15%）、財務・経理部門出身（15%）、本社スタッフ部門出身（10%）などとなっている。

IT部門出身でなく経営戦略や事業実態を理解した人材をCIOに任命するケースが多いのは、それだけ経営トップが経営とITの関係を重要視していることの表れともいえる。しかし、ITの専門家ではない経営幹部がCIOを務めるケースなどでは、何をどうすればよいか戸惑うことも少なくない。

経営幹部育成のための各種講座を開いている野村マネジメント・スクールはNRIと共同で、2011年11月から新たに「経営者のためのITマネジメント講座」を開設する。米国のビジネススクールの教授とNRIの専門家がクラス討議をリードし、経営者に必要なITの統制力や判断力を磨く講座である。企業の具体的なITの問題を事例にケーススタディーの形で授業を行うので、経営幹部やCIOの方々にはぜひ受講されることをお薦めしたい。

また、NRIは「経営戦略におけるITの位置づけに関する実態調査」を2008年から実施している。経営施策においてIT活用とその効果に何を期待するかを聞くと、①財務会計の適正化と迅速化に関わる仕組みの改善、②顧客情報や販売情報を収集し分析する機能の強化、③営業現場における情報活用力の強化―の順となった。②と③は、顧客接点での営業力・販売力を向上させることを目的としたもので、これを実現しようとすればCIOだけでなく経営企画や事業現場の中堅社員のIT活用スキルも高める必要がある。

事業現場で情報活用やIT活用のスキルを養い、次に情報システムの企画力や全社的なIT戦略の立案力を高めていくといった育成パスが重要である。そのエントリーコースとして、例えばITコーディネータ協会が作成した「IT経営体感ケース研修」を企業内研修に採用する方法も有効だろう。

経営戦略を実現する基盤でありツールでもあるITは、「どのように活用するか」が重要である。そのための鍵は人材の育成にある。ビジョンの実現に向けて熱い心で取り組むことに加えて、IT活用スキルを身に付けた人材をどう育て上げるか、そこに企業のIT経営の成否がかかっているといえないだろうか。■

複雑化する文書管理への対応
―体系的な情報セキュリティ対策の必要―

企業の中に蓄えられる文書は増加の一途をたどり文書管理が多様化・複雑化している。このためセキュリティの不備を招きかねない状況にあり、次々に登場する新しいメディアや機器への対応をどうするかも課題である。本稿では、複雑化する文書管理の状況を分析し、体系的でセキュアな文書管理のあり方を提言する。

複雑化する一方の文書管理

企業にとって、機密情報の漏えいは経営の根幹を揺るがす事態にもなりかねない重要な問題である。従って文書管理が企業の情報戦略の上で最重要課題となることは言うまでもない。それにもかかわらず、文書管理の方法やルールが不明確なままの企業が多いのも事実である。その最も大きな理由は、文書を格納する媒体が多様化し、行わなければならない管理の方法が複雑化していることである。

管理しなければならない対象は、紙の書類、キャビネットや机とその鍵、ノートPC、サーバー、記憶媒体（ハードディスク、USBメモリーなど）、さらにはネットワークからクラウドコンピューティング（以下、クラウド）にまで及ぶ。さらにスマートフォン（多機能な携帯電話）やタブレット型端末などの新しい機器やメディアへの対応も必要になる。

新しいデバイスの管理方法の例として、タブレット型端末の場合を考えてみよう。タブレット型端末は、可搬性が高い、大容量、見やすい、動作が速いなどのため爆発的に普及している。タブレット型端末は、大容量USBメモリー、ノートPC、ネットワーク端末という３つの観点から文書管理を考えなければならない。大容量USBメモリーは、厳格な持ち出し・返却記録と、承認および暗号化が必要である。ノートPCであれば、個人資産としての管理、利用ユーザー管理、パスワード管理も必要である。ネットワーク端末であれば、いつでもインターネットに接続できるため機密文書の電子ラベル付与などの対策が必要だろう。

急速に普及しているクラウドではどうだろうか。高価なコンピュータシステムを自前で保有して文書管理をするよりも、文書管理をクラウド上のサービスとして利用する方が経費節減につながる。しかし、クラウドで文書を保管することにはセキュリティ上の不安がある。パブリッククラウドでは文書は共有の仮想領域に格納されるため、この状態ではデータへの不正アクセスの可能性を排除できない。また、アクセス状況を把握するための証跡データが事業者から必ず提供されるとは限らない。ましてや文書を保存したサーバーが実際にどこにあるかが分からず、海外にあれば日本の法律を適用することは難しい。

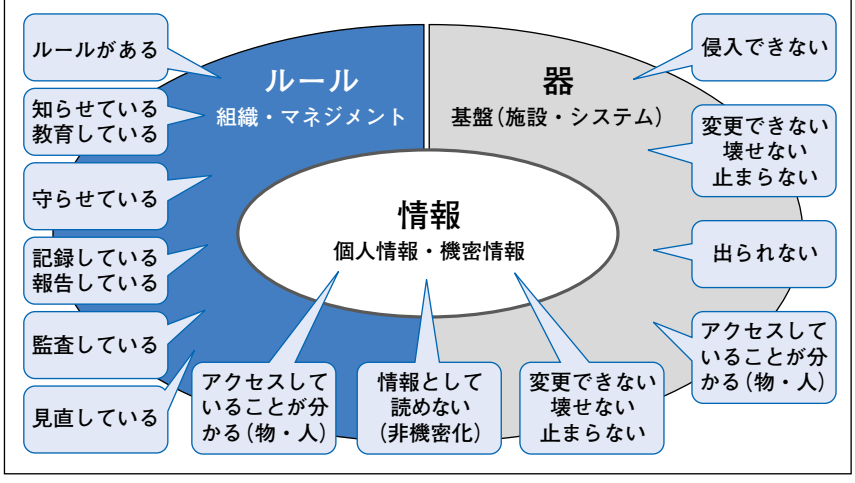
このように、文書管理のあり方は非常に複雑になっている。

野村総合研究所
情報セキュリティ部長
安田　守（やすだまもる）
専門はプロジェクト管理、セキュリティ管理、ソフトウェアエンジニアリング

文書管理の基本

複雑化する文書管理にどう対応すればよいだろうか。基本的には、管理対象を整理して体系的に対策を行うことである。そのためには、まず情報セキュリティで守るべきものは何なのかを考えることが必要である。

図1　情報セキュリティの概念



情報セキュリティとは、「情報（個人、機密）および情報を入れる器に対して、侵入、漏えい、改ざん、破壊、停止および不正への対策を行うこと、またこれらの対策（ルール）を周知徹底して機能させ、安全性を担保すること」である。すなわち情報セキュリティは情報に加えてその入れ物である器を守り、そのための方法をルール化してこれを徹底することである。情報はそのまま文書と読み替えることができる。

例えば重要な秘密情報があるとする。この情報が紙に記載されれば書類となり、PCのソフトウェアで作成されれば電子ファイルとなる。これが器である。書類を入れる机や、ファイルを格納する文書サーバーも器であり、それらが設置されている事務所の建物も器である。机の引き出しは施錠して鍵を所有者が管理する、文書サーバーにはアクセス権を設定して承認されたアクセスのみ許可する、オフィスの入退館時は警備員に入館証を提示するなどの決まりがルールである。この概念を示したのが図1である。

階層を意識した文書管理の具体化

体系的な文書管理とは、情報・器・ルールの階層ごとに、図1で示したセキュリティ対策を具体化することである。情報のレベルで文書を暗号化すればそのファイルは非機密化される。文書の改ざん防止のためにタイムスタンプを付与する方法もある。すべての文書を同じように管理するのではなく、電子ラベルによって機密度のレベルを決め、管理対象を絞ることもできる。こうした方法により、文書を対象としたセキュリティ対策の過不足や不備を把握でき、最適なセキュリティ環境を構築できるようになる。 ■

重要情報資産の所在管理のポイント
―ISO 27001認証取得企業の実例から―

情報セキュリティ管理に関する国際標準規格ISO 27001（JIS Q 27001）の認証取得を目指す企業が増えている。しかしその前提となる「情報資産台帳」を適切に作成することは実際には難しい作業である。本稿では、ISO 27001認証取得企業への聞き取り調査に基づいて、情報資産管理の課題を検討するとともに、これを効果的に解決するソリューションを紹介する。

実態とかい離する「情報資産台帳」

ISO 27001は、従来のISMS（情報セキュリティマネジメントシステム）を国際標準規格化したものである。ISO 27001の認証取得には、「リスクの洗い出し、定量化」が重要なポイントになる。その前提となるのが、重要度を識別した情報資産・電子ファイルをリストアップすること、すなわち「情報資産台帳」の作成である。特に、顧客情報や個人情報は徹底した管理下に置く必要がある。「情報資産台帳」の作成は、ISO 27001の認証とかかわりなく、一般の企業においても必要な作業であろう。

しかし電子ファイルは日々新たに作成され、内容が変更され、そして所在場所が変わることが多い。そのため「情報資産台帳」を作成してもすぐに実態と異なったものになってしまう。これは情報資産管理の難しさの1つである。実際にISO 27001の認証取得企業からも以下のような声を数多く聞いた。

①各部署のセキュリティ担当者が、それぞれの部署の個人情報ファイルの「情報資産台帳」を作成しているが、基本的にすべて手作業であるため、担当者の負担が大きく不満の声が上がっている。

②作成された「情報資産台帳」に間違いや不足があり、信ぴょう性が疑われるケースがある。

③「情報資産台帳」をしっかりと作成したつもりなのに、認証取得の審査員から内容がずさんだという指摘を受けた。

これらの声は、「情報資産台帳」による情報資産の所在管理がいかに難しいかを表している。これはISO 27001の認証取得に限らず、個人情報保護法やプライバシーマークへの対応などでも同様であろう。

文書機密度の判断の難しさ

情報資産に対する機密度は、文書に付与されたラベルで識別され、どういう文書に対してどのラベルを付与すべきかというルールが決められている。これまで筆者が見た例では、機密度ラベルには「極秘」「社内秘」「公開情報」や、「S」「A」「B」「C」などのアルファベットが使われることが多い。

このようなルールの策定や、社員に対するルールの徹底は、多くの企業では総務部門やコンプライアンス（法令遵守）推進部門などが担っている。

NRIセキュアテクノロジーズ
ソリューション事業推進部
セキュリティコンサルタント・CISSP
船越洋明（ふなこしひろあき）
専門はセキュリティ製品のプロダクトマーケティング

ルールを策定して文書へのラベル付与を徹底させようとした場合、ラベル付与が強制的に行われる何らかの仕組みがないと、ルールがあってもその運用が形がい化してしまうことは少なくない。筆者も「ルール自体の存在が忘れ去られている」という企業の声を聞くことがある。そうなると、ISO 27001に対応するために総務部門やコンプライアンス推進部門の担当者がラベル付与を行わなくてはならなくなってくる。

ところが同じ機密情報といっても、営業部門の機密情報と開発部門の機密情報では機密の尺度が異なることが多いため、機密度を部外の者が判断することは簡単ではない。「本来は、それぞれの社員がルールに従って日々の業務として機密度の識別（ラベル付与）をすればいいのだが、実際には現場部署に対して業務の合間に識別してくれるよう依頼するところから自分の仕事が始まる」と訴えるコンプライアンス推進の担当者もおり、苦労のほどがうかがえる。

台帳作成を自動化するソリューション

NRIセキュアテクノロジーズは、上記の課題を解決する情報資産識別・整理ソリューション「SecureCube／Labeling」のPersonal版を2009年10月から無償提供し、2010年２月からはPersonal版の有償サポートと、サーバー向けEnterprise版の販売を開始している。これによって、文書を保存する時に機密度に応じたラベル情報を強制的に付与し、その情報に基づいて自動的にファイル管理台帳を作成することができるようになる。以下では２つの主要な機能を紹介する。

①日次・週次・月次で台帳情報を生成

「SecureCube/Labeling」がインストールされたPCやファイルサーバー上では、日次・週次・月次のいずれかで自動的に台帳を作成し、管理サーバー内のデータベースに蓄積する。そのため、「情報のリストを３日以内に取引先企業に提出する」などといった場合でも、データベースから情報を抽出するだけですぐに対応できる。

②機密度以外の情報も付与

2011年３月にリリースした最新版では、金融庁による文書管理に関する指示があった金融業界を中心に要望が強かった「機密度以外の情報の付与（属性管理追加）機能」が搭載された。これにより、「極秘」「社外秘」以外に、「作成部署」「有効期限」などの情報も強制的に付与させることが可能になり、情報資産管理の粒度の向上が図られている。これらの情報は台帳にも反映されるため、きめ細かい台帳化と、台帳に記載された情報を検索する際の精度の向上が期待できる。

「SecureCube／Labeling」は、ラベル情報の強制的な付与、各種属性情報の追加、日次・週次などタイムリーな台帳生成などを実現することにより、多くの企業の情報資産管理を支援できるものと確信している。 ■

“環境管理型”情報漏えい対策の重要性
―セキュリティと利便性を両立させた暗号化ソリューション―

なぜ情報漏えい事故はいつまでもなくならないのであろうか。情報漏えい対策ソリューションの選択肢は増えているにもかかわらず、情報漏えい事故は減るどころか増加傾向にある。本稿では、ヘルスケア分野での情報漏えい対策ソリューションの導入経験に基づいて、企業の現実を見据えた情報漏えい対策、特に暗号化による対策について考察する。

増える情報漏えい事件

世の中にはさまざまな情報漏えい対策ソリューションがあふれている。それにもかかわらず、情報漏えい事件はなくなるどころか増加傾向にある。なぜ情報漏えいは減らないのだろか。

図１は、アイティメディアが公開している、情報漏えいの原因について2010年に行われた調査の結果である。PCやUSBメモリーの紛失など、上位にあげられる原因に共通しているのは、それが人為的なミスによるものだということである。これに比べて外部からの攻撃などは割合としては小さい。人的ミスを完全になくすことはできない。このことが、情報漏えいが減らない大きな要因の１つである。

情報漏えいが減らないもう１つの要因は、情報共有がますます進んでいることである。情報は、それが共有されることによってさらに価値が高まる。企業にとっては、社内で情報を共有し、組織の生産性を高めることはますます重要になっている。

情報を共有する人間が多数おり、人間は必ずミスを犯すという単純な事実が、情報漏えいがいつまでもなくならないことの背景にある。従って、情報漏えい対策にとって肝心なことは、人的ミスの発生を前提とすること、および情報共有の妨げにならないことである。

筆者はヘルスケア分野のシステム導入を専門としている。この分野は医師や患者の個人情報が多く扱われるため、情報漏えいには特に気をつけられている。以下では、野村総合研究所（NRI）がある製薬企業に対して行った情報漏えい対策ソリューション導入の経験に基づいて、あるべき情報漏えい対策について考える。

これまでの情報漏えい対策の問題点

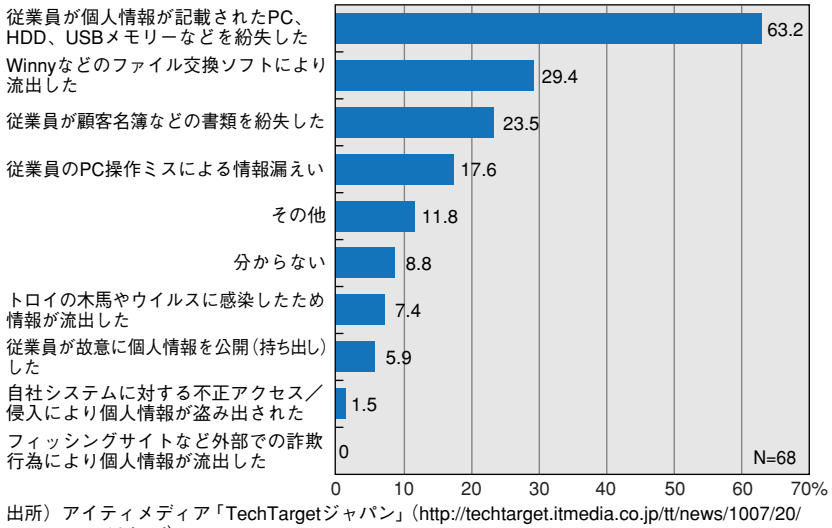
情報漏えい対策として最も一般的なのは、「アクセス権管理」と「暗号化」という２つの方法である。

アクセス権管理は、組織別、機密レベル別のアクセス制限が一般的である。各社員がアクセスできる情報を最小限にすることにより、情報漏えいのリスクは確かに減らすことができる。しかし、少数とはいえ、機密情報にアクセスできる社員がミスによって情報漏えいを起こす可能性は残る。また、リスクを小さくしようとすればするほど情報共有の範囲が狭くなり、組織としての生産性は低下する。

野村総合研究所
ヘルスケア・ERPソリューション事業本部
ヘルスケアシステム開発部
主任システムエンジニア
末廣信太郎（すえひろしんたろう）
専門はヘルスケア領域の情報系システム開発

暗号化は、どの部分で暗号化を行うかが問題になる。PCのハードディスクやUSBメモリーなどの機器レベルでデバイスを丸ごと暗号化する対策は一般的になってきている。これは機器の紛失による情報漏えいに対して一定の有効性はあるが、中身のファイルを持ち出されてしまうリスクはなくならない。

図1　情報漏えいの原因



出所）アイティメディア「TechTargetジャパン」（http://techtarget.itmedia.co.jp/tt/news/1007/20/news03.html）

最も確実な方法は、個々のファイルを暗号化することである。ファイルそのものが暗号化されていれば、たとえ持ち出されたとしても情報漏えいは防げる。しかし、ファイルを1つ1つ暗号化する方法では暗号化をし忘れる危険もあり、また権限を設定された人間やパスワードを知っている人間しかアクセスできないため情報共有の範囲が限定される。

複数のソリューションを組み合わせる

上記のように、アクセス権管理、暗号化のどちらも有効な対策ではあるが、それだけでは人的ミスによる情報漏えいを完全には防げず、情報共有の範囲も狭めることになる。

人的ミスの発生を前提とし、情報共有を妨げない単一のソリューションを見つけることは難しい。そのため、複数のソリューションを組み合わせてこれを実現する必要がある。筆者らが採用したのもこの方法である（次ページ図2参照）。

(1) ファイルの自動暗号化

ミスが起きても情報漏えいが起きないようにするためには、暗号化が自動的になされなければならない。筆者らは、製薬企業での情報漏えい対策として、米国Microsoft社のグループウェア「Microsoft Office SharePoint Server」（以下、SharePoint）と暗号化ソリューション「Windows Rights Management Services」（以下、RMS）を組み合わせたソリューションを選定した。

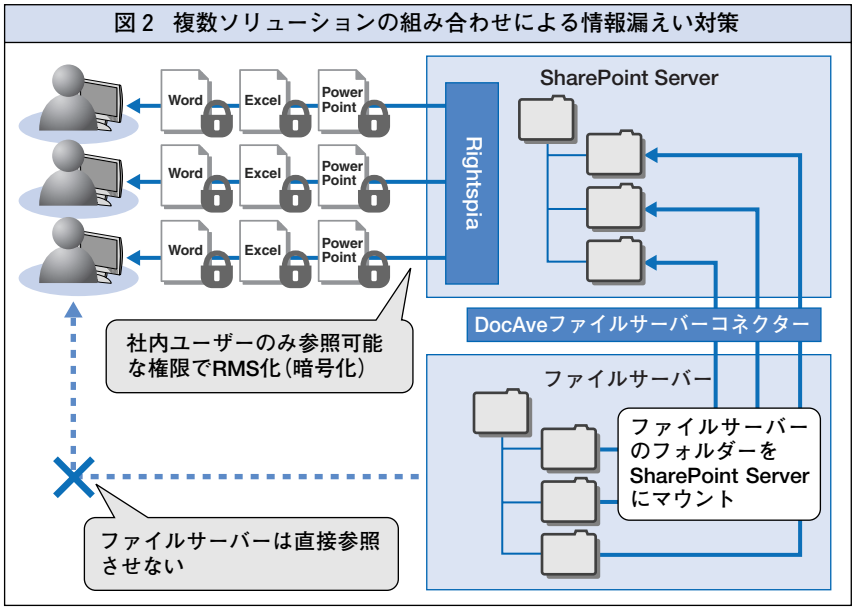
SharePointは企業内の情報共有基盤として普及しつつある製品である。通常のWindows上のフォルダーにアクセスするのと同じ感覚

で、ファイルサーバーのようにSharePointを利用することが可能である。

暗号化の対象となるのはSharePoint内のMicrosoft Officeファイルで、これを取り出す際に自動的にRMSで暗号化される。

RMSで暗号化したファイルは、権限を持つユーザーのみが開くことができる。暗号化ファイルを開く際には、PCへログインした時に権限が判断されているのでパスワードを入力する必要はない。移動の最小単位であるファイルそのものが自動的に暗号化されるため、例えば電子メールの誤送信などで意図せずファイルが流出しても、情報漏えいが起きるリスクは格段に低い。

図２　複数ソリューションの組み合わせによる情報漏えい対策



(2) 情報共有を妨げない

先に述べたように、暗号化は情報漏えいを防ぐことはできても情報共有を妨げるというジレンマがある。この点ではSharePointとRMSによるファイルの暗号化も課題を残している。SharePointの暗号化機能では、ファイルを開けるのはダウンロードした本人のみであるため、ファイルを社内の別ユーザーと電子メールなどで共有するといったことができないからである。

これを解決するため、筆者らは「社員のみ開ける形での暗号化」を実現した。フォルダーなどの単位で適切なアクセス権管理を行っていれば、ファイル単位の暗号化時に細かく権限を制御する必要性は低い。従って、暗号化は社外への情報漏えい対策と割り切り、社員であれば暗号化を意識せずにファイルを開けるようにしようという考え方である。具体的には、ファイルを暗号化する際の権限設定を変更するソリューション（富士通エフサスの「Rightspia for Secure Documents」）をSharePointと組み合わせることによって実現した。

(3) 大量の既存ファイルを新基盤に移行

情報漏えい対策を真に有効なものとするためには、もう１つ大きな課題がある。それは、大量の既存資産すなわち既存の多数のファイ

ルサーバーと、その中の膨大なファイルをどう守るかということである。

ファイルサーバーは、ほとんどの企業で利用されている情報共有手段であるが、情報量が増えるにつれて必要な情報を見つけにくくなり、活用されないファイルが削除されずにひたすら蓄積されていく傾向がある。大きな問題は、活用されない大量のファイルの中に機密情報や個人情報が含まれ、情報漏えいのリスクが放置されていることである。筆者らが情報漏えい対策ソリューション導入に際して直面したのも、大量の既存資産をどうするかという問題であった。大量のファイルを別基盤に移行するのは非常に時間のかかる作業だからである。

筆者らはこの問題を解決するために、従来のファイルサーバー上のファイルを残したまま、ファイルにアクセスするための入口のみSharePointに置き換えることにした。採用したのは米国AvePoint社の「DocAve」である。これにより、新システムへの移行時間を大幅に短縮することができた。また、利用されていないファイルを一定期間後に自動削除するようにした。

セキュリティ対策は“環境管理型”へ

セキュリティ対策を強化すると、「不便」や「面倒」といった声が社員の間から聞こえてくることがある。これはセキュリティ対策を強いられる社員の本音であろう。セキュリティのために、従来の業務にさまざまな手続きが付け加わり、業務効率や利便性が犠牲にされる。問題が起きるたびにルールや手続きが増え、社員の仕事は増える一方である。

ルールを作り、そのルールを守るよう社員を訓練・監視する従来の“規律訓練型”のセキュリティ対策はもう限界に来ている。これからは、“環境管理型”セキュリティ対策への移行が必要である。

環境管理型セキュリティ対策とは、社員がその環境内で自由に活動しても結果的にセキュリティが守られるような環境を作ることである。忘れてならないのは、セキュリティ対策は企業のビジネスにとって本業ではないということであり、セキュリティのために本業の業務効率が下がることがあってはならない。ソリューションの選択肢が増えている今、複数のソリューションを適切に組み合わせて、利便性とセキュリティを両立させた環境を実現することが可能になってきている。

このような環境を実現するためには、部分最適に陥ることなく、社員を取り巻く環境全体を最適に設計する幅広い視点が必要である。同時に、新しいソリューションを組み合わせる際に起こりやすい問題にも注意を払う必要がある。

本稿で紹介した環境管理型のセキュリティ対策ソリューションが、今後の情報漏えい対策の大きな流れとなっていくことは間違いないであろう。 ■

電子データの存在日付を公的に証明
―電子タイムスタンプサービス「Cyber Date Stamp」―

企業が自社の技術を特許化（技術の公開）せずにノウハウとして秘匿する際に、その技術がいつから存在するかを証明し、それが変更・改ざんされていないことを客観的に担保する「電子タイムスタンプ」を利用する動きが広がっている。本稿では、NRIサイバーパテントが提供する「Cyber Date Stamp」を紹介し、効果的な電子タイムスタンプの活用について提言する。

戦略的な知的財産管理のために

近年、国際的な企業間競争がますます激しくなっている。企業は自社が開発した技術について、公開が前提となる特許出願をするか、あるいは社内のノウハウとして秘匿するか、戦略的な知的財産管理を行っていくことが重要になっている。

特許出願を選択した場合、出願公開制度により出願日から１年半で自動的に出願内容が公開される。特許出願により、権利化できるメリットと引き換えに、自社の技術が公開されることで競争力を損なうリスクが生じる。また、出願に係る費用や、審査に時間がかかることも特許取得の問題点である。一方、ノウハウとして秘匿することにした場合、技術公開によるリスクを低減できる代わりに、他の企業に同技術の特許を取得されるリスクが生じる。従って、これらのメリット、デメリットを考慮した上で特許出願を検討することが企業には必要になっている。

「先使用権」確保の重要性

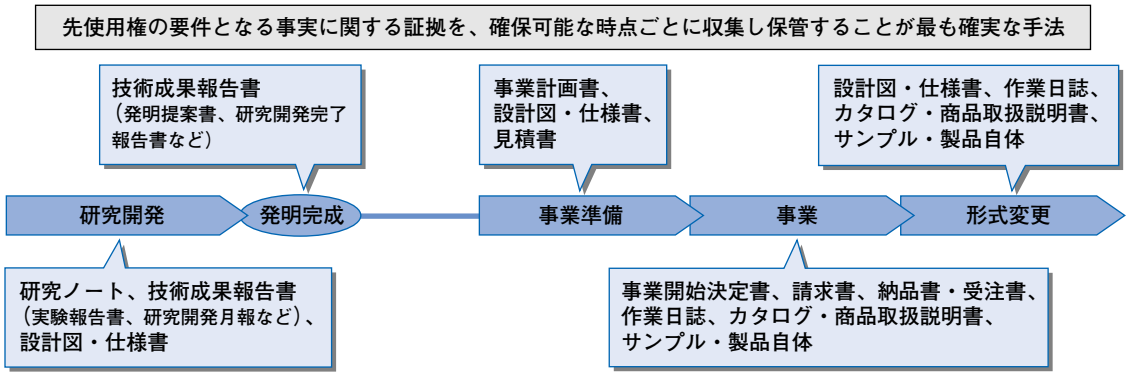
世界の主要国の特許制度は、複数の者が独立に同一内容の発明をした場合には、先に特許出願した者（先願者）だけが特許権を取得できる先願主義を採用している。

先願主義の原則を貫くと、先願者が特許出願を行う前から同一の技術に基づいて事業を行っていた者あるいは事業を準備していた者（先使用者）は、先願者が権利を取得してしまえば事業を行えなくなる。このような事態を回避し、特許権者と先使用者の公平を図るために、法律の定める一定の範囲において先使用者が引き続き事業を継続できるようにするための「先使用権」制度が用意されている。先使用権の確保は、自社の技術を特許出願せずにノウハウとして秘匿するための重要な手段である。

先使用権を行使するためには、自社が使用する技術がいつから存在したかを証明する必要がある。そのために、従来は公証役場にて技術内容が記載された紙媒体や電磁的記録媒体に日付証明を受ける必要があった。しかしこの方法は、文書を印刷して公証役場へ持参したり、電子ファイルの媒体を複製して保管したりする必要があるなど、機動性や管理の面で課題がある。また、あらゆる業務で文書の電子化が進んでいる今日では、膨大な電子的文書の作成日付管理を適切に行うことも大

NRIサイバーパテント
知的財産情報サービス事業部
新妻信人（にいづまのぶと）
専門は知的財産関連サービスの企画・営業

図1　知的財産情報の生成と先使用権確保の考え方



出所）特許庁総務部企画調査課「先使用権制度の円滑な活用に向けて一戦略的なノウハウ管理のために一」
（http://www.jpo.go.jp/torikumi/ibento/text/pdf/h19_jitsumusya_txt/senshiyouken-toujitsu.pdf）

きな課題になる。

電子タイムスタンプへの期待

技術内容が記載された知的財産情報は、構想から実施までの一連の過程で作成される多数の資料から成り立っている（図1参照）。これらの知的財産情報を迅速に収集・記録・保管し適切に管理するために、文書の電子化は最適な手段である。しかし、通常、電子データは変更が容易な上に改ざんなどの痕跡も残らない。従って、いざ係争となったとき、先使用を立証するのは困難である。

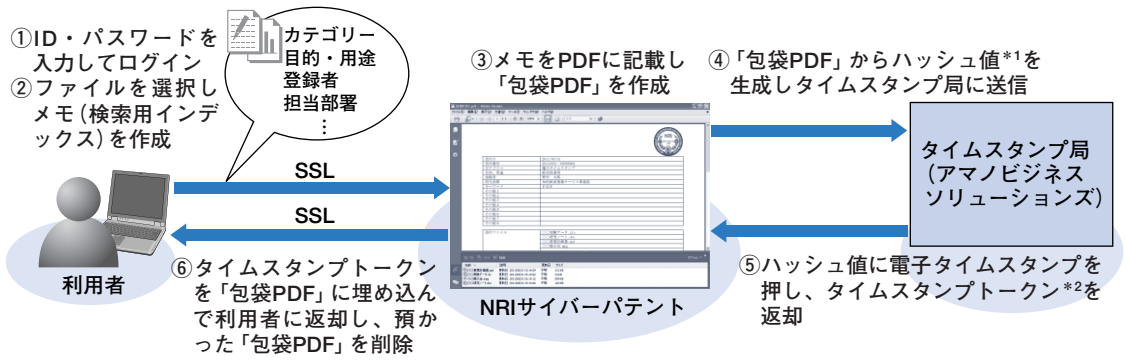
この問題を解決するために浸透しつつあるのが、PCなどの内部時計ではない“正しい時刻情報”（タイムスタンプ）を電子データに付与する電子タイムスタンプの仕組みである。電子タイムスタンプは、電子データが格納された媒体に対してではなく、データそのものにタイムスタンプを押す。タイムスタンプが付与された時点でそのデータが存在したことが証明されるとともに、その時から現在まで内容が変更されていないことも同時に証明される。電子タイムスタンプは、特許庁が2006年に公開した先使用権制度に関するガイドラインの中で、先使用権行使の具体的手法の1つとして推奨している。今後、業種を問わず知的財産権の確保のために採用が進んでいくと予想される。

電子タイムスタンプは以下の要件を満たすことで信頼性が担保される。

①信頼できる時刻源の確保

時刻を証明する役割を持つタイムスタンプ局（TSA：Time-Stamping Authority）の時刻が国家時刻標準機関（NTA：National Time Authority）の時刻源に基づいていること、もしくはNTAの時刻源に基づいた時刻を時刻配信局（TA：Time Authority）から配信されていることを証明する。

図２　「Cyber Date Stamp」の仕組み



*1：電子ファイルから固定長の疑似乱数を生成する演算手法により生成した値。ハッシュ値から元のファイルを復元することはできない。2つの異なるファイルから同じハッシュ値を生成することは極めて難しい。
*2：ハッシュ値に電子タイムスタンプを付与したもの。
※「Cyber Date Stamp」は野村総合研究所グループの登録商標
※「包袋PDF」はアマノおよびアマノビジネスソリューションズの商標

②非改ざん性（完全性）の保証

暗号技術を用いていることで、電子署名と同様にタイムスタンプが付与されたデータおよびそのタイムスタンプが改ざんされていないことを証明する。

「Cyber Date Stamp」サービスを提供

これまで、電子タイムスタンプを利用するためには、利用者のPCに専用ソフトをインストールするか、または専用サーバーを導入することが必要であった。また、タイムスタンプを押したいファイルが複数ある場合は、それぞれのファイルに電子タイムスタンプを押す必要があるなど利便性の面で課題があった。これらが、電子タイムスタンプの普及を妨げていたといえる。

そこでNRIサイバーパテントは、これらの課題を解決することによって電子タイムスタンプをより利用しやすくするために「Cyber Date Stamp」を2010年８月から提供している（図２および図３参照）。

「Cyber Date Stamp」の主な特徴は以下のとおりである。

①専用ソフトのインストールが不要

標準的なWebブラウザーを通じて利用でき、専用ソフトをインストールする必要がない。インターネットに接続できる環境があれば、すぐにサービスを利用できる。Webブラウザーから「Cyber Date Stamp」のサイトにアクセスし、IDとパスワードを入力してログオンする。次にタイムスタンプを付与したいファイルをサーバーにアップロードする。これだけの手順で簡単に電子タイムスタンプを付与することができる。

②複数ファイルに一括してスタンプを付与

PDFのファイル添付機能を利用して複数の

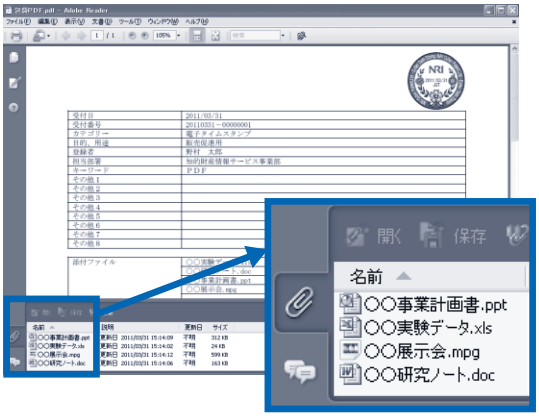


図 3 「包袋PDF」ファイル

ファイルをまとめてPDFファイルに添付し、PDFファイル単位で電子タイムスタンプを付与することが可能である。電子タイムスタンプは、業務で使われることの多いMicrosoft社の「Word」「Excel」「PowerPoint」のほか、動画や音声を含むあらゆるアプリケーションソフトのファイルに付与することができる。ファイルをサーバーにアップロードする際の通信手順にはSSL（Secure Sockets Layer：WebブラウザーとWebサーバー間で安全にデータ通信を行うためのプロトコル）を使用して安全性を確保している。

③スタンプ付与ファイルの管理・検索

「Cyber Date Stamp」では、アップロードする複数のファイルをまとめてPDFファイルに添付する際、このPDFファイルにカテゴリー区分やキーワード、タイムスタンプ付与日などのインデックスを付与することができる。これにより、タイムスタンプを付与したファイルの管理・検索が容易になる。

広がる電子タイムスタンプの用途

「Cyber Date Stamp」は、生産ノウハウなどの先使用権を確保したいという理由から、これまで大手化学品や食料品製造業を中心に導入されてきたが、最近は他の業種にも広がりつつある。

電子タイムスタンプはさまざまな目的で活用できる。例えば共同研究において権利関係の持分や研究成果の貢献度などで争いになった場合、事前に自社に関連する技術資料に電子タイムスタンプを付与しておくと、そうしたトラブルを回避することが可能になる。

このほか、契約書や提案書など日常的に作成される各種文書なども、電子タイムスタンプを付与しておくことによって、係争になった場合に有効な証拠となり得る。また財務省や国立印刷局でも、証書や官報に電子タイムスタンプを付与する取り組みを進めている。

「Cyber Date Stamp」では最大1GB（ギガバイト）のファイルに電子タイムスタンプを付与することができるため、音楽・映像作品など著作権分野での広がりも期待できる。

NRIサイバーパテントは、長年にわたって蓄積してきた知的財産分野でのノウハウを基に、企業における電子タイムスタンプの活用を知的財産の特性に応じて効率的かつ効果的にサポートするため、タイムスタンプの有効期限の管理や自動更新など、さまざまなソリューションを検討している。 ■

IT化によるコミュニケーション重視の営業が求められる金融機関

金融機関が“顧客経験価値”の向上を図るなか、信用金庫などの“顧客密着力”があらためて注目されている。店舗窓口や営業担当者の顧客接点における“ハイタッチ”な（コミュニケーション重視の）営業力を強みとする信用金庫は、大手銀行、地方銀行などからの資金流入も増えている。本稿では、ITを活用した“ハイタッチ”なサービスの可能性について考察する。

顧客接点が弱まった大手・地方銀行

大手銀行や地方銀行では、手数料優遇などによって顧客の取引をATMやネットバンキングなどの非対面チャネルに誘導し、コスト削減や窓口業務の効率化などを図ってきた。しかしその結果、店舗に顧客が来店する機会が減り、顧客とのコミュニケーションに基づいた営業力が弱まったという話をよく聞く。

野村総合研究所（NRI）の「生活者１万人アンケート調査（金融編）」では、信用金庫・信用組合をメインの金融機関（最も多く資産を預けている金融機関）にしている人が対面チャネルを利用する割合（非対面チャネルとの比較）は、大手銀行や地方銀行をメインにしている人より高いという結果が出ている。

例えば、東京都の巣鴨信用金庫は“ホスピタリティバンク”を標榜し、電話一本での訪問、休日夜間の住宅ローン相談、ATMコーナーでの19時までの通常窓口業務、年金無料宅配、支店での区民サービスコーナーの設置など、対面でのさまざまなサービスを提供している。この実例と上記の調査結果を考えると、信用金庫・信用組合では対面の顧客接点が維持されていると見てよいのではないだろうか。

信用金庫・信用組合への資金流入

信用金庫の預金残高も増加し続けている。全国272の信用金庫（2010年12月末時点）の譲渡性預金を除いた預金残高は、いわゆる団塊世代の退職金や年金振込などの要因により、2010年12月末で120兆円を突破している。金融専門紙『ニッキン』の2011年２月４日の記事によると、1997年12月に預金残高が100兆円を突破してから2005年12月に110兆円に到達するまでに８年を要したのに比べ、120兆円の到達は５年で達成しており、信用金庫業界の預金量は順調に拡大しているという。

前述の「生活者１万人アンケート調査（金融編）」では、定期預金の預け替えが、どの金融機関からどの金融機関に対して行われたかも聞いている。それによると、信用金庫・信用組合は流入額が流出額より多く、しかも、大手銀行・ゆうちょ銀行・地方銀行のいずれからも流入超の状態である（図１参照）。

アンケート調査では、借入金額が最も多い住宅ローンを他の金融機関から借り替えた人数も調べており、ここでも信用金庫・信用組合は流出より流入が多くなっている。

このように、定期預金や住宅ローンなどの

野村総合研究所
システムコンサルティング事業本部
ビジネスデザインコンサルティング部
主任システムコンサルタント
北野貴之（きたのたかゆき）
専門は金融機関のマーケティング戦略策定支援・
システム開発プロジェクトマネジメント支援など

サービスにおける顧客獲得の面では、信用金庫・信用組合は一定の成功を収めている。

ITで実現する“ハイタッチ”営業

顧客との対面の接点を重視した信用金庫・信用組合の“顧客密着力”は、顧客経験価値を高め競争力を強化するための注目すべきポイントである。顧客と密にコミュニケーションをとり、顧客を知り尽くした人間関係重視の“ハイタッチ”な営業力こそ、信用金庫・信用組合に個人顧客の資金が流入している大きな要因と思われる。

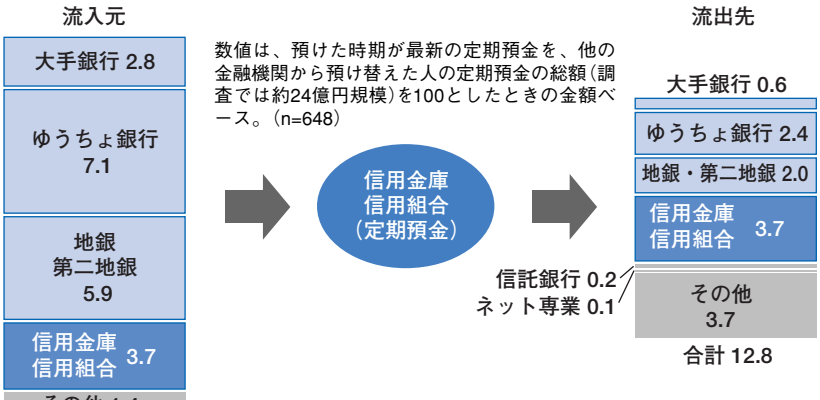
このような“ハイタッチ”な営業は狭域高密度の態勢であるほど可能と考えられる。前述の巣鴨信用金庫のサービスも、営業範囲が狭いために実現できるものであり、大手銀行や地方銀行などが同様のサービスを提供しようとしても、効率やコストの面で実現可能性は低い。従って、大手銀行や地方銀行などが顧客経験価値の高い“ハイタッチ”なサービスを提供するためには、ITを活用したサポートがどうしても必要である。

まず、店舗の窓口や営業担当者などの対面チャネルと、コールセンターやインターネット、ATMなどの非対面チャネルのどちらでも一貫性のある顧客サービスを提供できるよう、各チャネルでの顧客とのコミュニケーションを統合するための仕組みが必要である。

営業担当者の営業活動においては、定期預金の満期のお知らせ、投資信託や社債の償還・分配金支払いなど、期日管理をサポートするシステムが必要となる。また、そのようなタイミングに合わせて、顧客が価値を感じられるサービスや商品を提案できるよう、相談業務をサポートするエージェント機能も有効と考えられる。

金融機関の従来の強みは、顧客サービスを提供する最終的な接点である窓口や営業担当者などの対面チャネルであったはずである。その活動の精度や対面以外の顧客接点との一貫性をITによりサポートしていくことで、効率的に“ハイタッチ”なサービスを提供できるようになると思われる。■

図1　信用金庫・信用組合の定期預金の流出・流入先



注1：自由記述された金融機関名を含まない集計。
注2：大手銀行は三菱東京UFJ銀行、みずほ銀行、三井住友銀行、りそな銀行。

業務アウトソーシングを拡大する欧米の資産運用会社

欧米の資産運用会社は、自社の最重要業務へ重点的に経営リソースを配分するため、本業以外の業務をアウトソーシング（外部委託）することが多い。いまでは、業務リスクの高い“ミドルオフィス業務”にまでアウトソーシングの範囲は拡大するようになってきた。本稿では、欧米の資産運用会社のアウトソーシングの事例を紹介し、今後の展開を予想する。

限定的だったアウトソーシングの範囲

資産運用会社の業務は、一般にフロントオフィス業務、ミドルオフィス業務、バックオフィス業務の３つに大別できる。中でも投資業務を行うフロントオフィス業務は資産運用会社の「本業」と位置づけられることが多い。

一方、ミドルオフィス業務とバックオフィス業務は、一般にフロントオフィス業務と比較すると他社との差別化をしにくく、アウトソーシングに向いている。特に基準価額計算などのバックオフィス業務は、特定のルールが存在することから定型化が進んでおり、アウトソーシングが比較的容易である。そのため欧米では資産運用会社が本業以外の業務をアウトソーシングするケースが多く、2000年以降はアウトソーシングの範囲をミドルオフィス業務へと広げる傾向が強まっている。

しかしその一方で、アウトソーシングの拡大に踏み切れない運用会社も多い。この数年、投信関連業務がヘッジファンドや機関投資家向けに月次や日次ベースで行われるようになった影響で、時価評価、パフォーマンス評価、ファンドのポジション管理などを含め、ミドルオフィス業務はきめ細かいシステムのモニタリングなどが必要となり、その業務リスクは高まっている。このリスクの高さゆえに、顧客レポート、パフォーマンス測定やコーポレートアクションに関する業務などは外部には任せられないと考える資産運用会社が従来から多かった。

リスクの高い業務のアウトソーシング事例

ミドルオフィス業務の中でも、コーポレートアクションに係わる業務は特にリスクが高く、アウトソーシングしにくい業務の１つといえる。コーポレートアクションは企業の株価や社債の価値に影響を及ぼすため、運用会社にとって極めて重要な情報であることも第三者に任せにくい理由である。そのため、最近のある米国での調査によれば、アウトソーシングを行っている運用会社は32％に過ぎず、まだ少数派である。しかし、近年、米国ではコーポレートアクションに関連するすべての業務をカストディアン（有価証券の保管管理業務を行う金融機関）へアウトソーシングする運用会社が出てきた。ここ数年、コーポレートアクションの種類が増え、その中身も複雑になってきており、業務負担が増えているからである。アウトソーシングを検討する運

NRIアメリカ
リサーチアナリスト
三上直美（みかみなおみ）
専門は米国金融サービス調査

用会社が増えてきているものの、このような事例は先進的であり、ある意味では大胆な取り組みとして注目できよう。

このアウトソーシングを実現した背景として、サービス提供側がカストディアンであったことがポイントと筆者は考えている。カストディアンのサービスは本来、有価証券を確実に保管し管理することだが、このアウトソーサーは有価証券に係わるコーポレートアクション情報の報告事務をサービスしてきており、そのための業務プラットフォームシステムの開発に必要な能力はすでに持っていた。また、長年の運用会社とのビジネス上の関係を通じて、コーポレートアクション関連の顧客要件をよく理解していたことも重要である。

この結果、アウトソーサーは運用会社の業務リスクを引き受ける代わりに、長年にわたって蓄積してきた業務ノウハウと、グローバルカストディアンとしての規模を生かしながら、一連の業務プロセスを有償のサービスにすることができたのである。

一方、アウトソーシングを選択した運用会社には次の３つのメリットがあった。

１つ目は、アウトソーサーが提供するプラットフォームシステムが成熟したことで、統合・標準化されたコーポレートアクション情報と、レスポンスおよび配当金の支払い情報をリアルタイムで確認でき、業務管理を実施できるようになったことである。

２つ目は、グローバルカストディアンであるアウトソーサーが、すでに新興国市場の情報の入手およびその事務処理を事業の一部としているために、自ら追加投資することなく価値の高い業務支援を期待できることである。

３つ目は、カストディアンで働く専門性の高い業務スタッフに、コーポレートアクション情報の検証作業を依頼できることである。これにより、株式公開買付のような複雑な選択権付きコーポレートアクションであっても確実に処理することができるようになった。

結果として、業務リスクからアウトソーシングをためらってきた運用会社も、適切なモニタリングなどを適宜行うことで、より安心して業務を行えるようになったのである。

能力の高いアウトソーサーの出現に期待

本業である投資リターンの追求をしながら、投資戦略や運用商品の多様化を図る欧米の資産運用会社は、これまで難しいと考えてきた、リスクの高い業務へとアウトソーシングの範囲を広げようとしている。現在、日本では、基準価額計算のようなバックオフィス業務を含め、業務のアウトソーシングは欧米ほど進んでいない。しかし日本でも、将来は受託能力の高いアウトソーサーが現れることで、リスクの高い業務を含むアウトソーシングが促進されると思われる。競争力の強化と効率化を追求する資産運用会社にとって、そのような選択肢が増えることは好ましい事業環境といえるだろう。 ■

NRI Web Site

■『ITソリューション フロンティア』本誌記事およびバックナンバーは、野村総合研究所（以下、NRI）ホームページで閲覧できます。
URL：http://www.nri.co.jp

■『ITソリューション フロンティア』に関するご意見、ご要望などは、氏名・住所・連絡先を明記の上、下記あてにお送りください。
E-mail：it-solution@nri.co.jp

NRIグループと関連団体のWebサイト

野村総合研究所
http://www.nri.co.jp

NRIネットワークコミュニケーションズ	http://www.nri-net.com
NRIセキュアテクノロジーズ	http://www.nri-secure.co.jp
NRIサイバーパテント	http://www.patent.ne.jp
NRIデータiテック	http://www.n-itech.com
NRI社会情報システム	http://www.nri-social.co.jp
ユビークリンク	http://www.ubiqlink.co.jp
NRIパシフィック	http://www.nri.com
野村総合研究所（北京）有限公司 上海支店	http://beijing.nri.com.cn http://shanghai.nri.com.cn
野村総合研究所（上海）有限公司	http://consulting.nri.com.cn
野村総合研究所（香港）有限公司	http://www.nrihk.com
NRIシンガポール	http://www.nrisg.com
NRIソウル支店	http://www.nri-seoul.co.kr
NRI台北支店	http://www.nri.com.tw
（財）野村マネジメント・スクール	http://www.nsam.or.jp

マッチング・ポータルサービス

B2Bポータルサイト「BizMart」	http://www.bizmart.ne.jp	情報収集、情報交換、商取引などの企業活動を総合的に支援する企業間ネットワークサービス

ナレッジ・ポータルサービス

NRIサイバーパテントデスク	http://www.patent.ne.jp	国内外の特許情報や主要企業の技術雑誌（技報）の検索・閲覧サービス
情報技術本部サイト	http://www.nri-aitd.com	最先端のITに取り組む技術集団である情報技術本部の活動内容や研究開発を紹介
日本企業台湾進出支援「ジャパンデスク」	http://www.japandesk.com.tw	台湾経済部と共同で、日本企業の台湾進出を支援

ソリューション・サービス

オブジェクトワークス	http://works.nri.co.jp	MVCモデルに基づくWebアプリケーション開発のためのJ2EE準拠開発フレームワークの紹介
BESTWAY	http://www.bestway.nri.co.jp	金融リテール投信ビジネスの“De-facto”スタンダードシステム。100社を超える金融機関が利用中
TRUE TELLER（トゥルーテラー）	http://www.trueteller.net	コールセンターからマーケティング部門まで、様々なビジネスシーンで活用可能なテキストマイニングツール
統合運用管理ソリューション（Senju Family）	http://senjufamily.nri.co.jp	NRIが培ったノウハウを結集した統合運用管理製品群。企業の「ITサービスマネージメント」の最適化を実現
PCLifecycleSuite	http://www.pcls.jp	企業内のPC運用コスト削減と品質向上を同時に実現する、PC運用管理の再構築サービス

インターネットリサーチ

TRUENAVI	http://truenavi.net	NRIが戦略策定等のコンサルティングに際して独自に開発したインターネットリサーチを企業向けに提供

ナビゲーションサービス

携帯電話の総合ナビサービス「全力案内!」（ユビークリンク）	http://www.z-an.com	携帯総合ナビサービス。世界初の携帯プローブ交通情報で道案内も。NTTドコモ、au、ソフトバンクから提供中

ITソリューションフロンティア

2011年5月号　Vol.28 No.5（通巻329号）
2011年4月20日　発行

発行人　嶋本　正
発行所　株式会社 野村総合研究所　コーポレートコミュニケーション部
〒100−0005　東京都千代田区丸の内1−6−5　丸の内北口ビル
ホームページ　http://www.nri.co.jp

発　送　NRIワークプレイスサービス株式会社 ビジネスサービスグループ
〒240−0005　横浜市保土ケ谷区神戸町134
電話（045）336−7331／直通　　Fax.（045）336−1408


NRI
未来創発
野村総合研究所