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「一歩先を行く情報セキュリティ」

07 | 2010 Vol.27 No.7
（通巻319号）

www.nri.co.jp

野村総合研究所
Nomura Research Institute

ITソリューション フロンティア
IT Solutions Frontier
07／2010

NRI Web Site

脳の進化とシステムの進化

人間の脳は、大脳辺縁系を中心とする“祖先型システム”（脳を持つ多くの動物に共通に見られる古い部分）と、その上に構築された大脳新皮質を中心とする“熟慮型システム”（人間の脳に特徴的な新しい部分）からできている。人間の脳は古いものに新しいものを重ねることによって進化したのである。

そんな脳を持った人間の論理的とはいえない行動をさまざまな視点から論じた興味深い本が、米国のゲアリー・マーカス著『脳はあり合わせの材料から生まれた』（2009/01、早川書房刊）である。

脳の大きな特徴は“Kluge”（クルージ）だという。“Kluge”は技術用語で、「エレガントにはほど遠く無様（ぶざま）であるにもかかわらず、驚くほど効果的な問題解決法」という意味である。その場しのぎの改変を重ねて、たまたまいまの形になったという脳がどのように“Kluge”なのか見ていこう。

例えば記憶である。記憶は海馬などの大脳辺縁系、すなわち祖先型システムと関係が深く、“文脈依存”の形をとる。コンピュータがメモリーの特定の場所に特定のデータを記憶（記録）するのに対して、人間の脳は過去の体験と似たような環境（文脈）に置かれると原記憶をよみがえらせる。

人間の思考は、この記憶システムをベースにしながら熟慮型システムも併用する。しかし、人の記憶は文脈依存型なので、コンピュータと違って信頼性に問題があり、正確性を欠いていることが多い。その上、ストレスなどの影響を受けると熟慮型システムは活動が鈍くなってしまう。そのため、人はしばしば間違った思考や推論をすることになる。これは、脳の進化が必ずしも最適化を意味しないことを表している。

物事の選択でも同様である。人間には未来よりも現在を重視する傾向がある。いまは我慢した方が未来に得られる効用が大きくなると分かっていても、いまの小さな利益を手に入れたがるのである。

これは「不確実性への適合」という進化の結果だという。現在を重視するのは祖先型システムであり、未来を考えるのは熟慮型システムだが、本能をつかさどるのは祖先型システムである。乏しい食糧という環境下で、不確実な将来のために種をとっておくよりも、いまそれを食べてしまうことで進化してきたのが人間なのだ。

このように書いてくると、祖先型システムには良いところがないように見えるかもしれないが、そうではない。祖先型システムは細部を分析的に見るよりも全体像をつかむのが得意であり、熟慮型システムは物事を１つ１つ解釈するのが得意である。このように違う特徴を持った２つのシステムが共存していることが問題なのではなく、２つのシステムの相互作用の仕方が問題なのだ。人間は心の悩

野村総合研究所
執行役員
基盤サービス事業本部長
情報技術本部長
綿引達也（わたひきたつや）

みが多いほど理性的な熟慮型システムが機能しなくなり、固定観念に染まり自己中心的になってミスを犯しやすくなる。けれども、祖先型システムをうまく使っていい結果を得ることもできる。

最近、プロの棋士が詰将棋を直感で解く時の脳の働きを観察する実験が行われた。その結果は非常に興味深いものであった。棋士の脳では、祖先型システムである辺縁系の大脳基底核と小脳が盛んに活動していたのである。定石を覚えたり対戦経験を重ねたりしながら強くなっていくのは熟慮システムのなせるわざであるが、その結果、祖先型システムが得意とする深い直観が身に付いていく。それは脳の古いシステムの再活用を意味しているのではないだろうか。

それでは、人間の脳に例えられることの多いコンピュータシステムの進化とはどのようなものだろうか。コンピュータシステムも、ビジネスの拡大やITの進歩によって常に進化を遂げてきた。この30年ほどを振り返ると、その進化は次の４つのパターンに大きく分けられると思う。

①追加型進化

従来のシステムをそのまま残しながら新しいシステムを追加する。

②モダナイゼーション型進化

従来のシステムのインフラを刷新し、その上で従来どおりの業務を行う。

③再構築型進化

業務の見直しを行い、従来のシステムをやめて新たにシステムを構築する。

④サービス型進化

従来のシステムをやめ、パッケージやネット上のサービスを利用する（業務はそれに合わせる）。

以上の４つの進化型にはそれぞれ長所と短所があり、どれが良いと一概にはいえない。

②③④はどれも進化のハードルは高いが、①は比較的容易である。脳は結果として①の道筋をたどって進化してきたが、“Kluge”となって問題も抱えることになった。

コンピュータシステムの進化が脳の進化と違っているのは、古いシステムを廃棄して一から作り直すことができる点と、進化の道筋を複数の選択肢から選ぶことができるという点である。

システムも単純な追加型を選べば“Kluge”なものとなり、脳のようにさまざまな問題を抱えることになる。しかし他の方向の進化のハードルは高い。ユーザー企業は明確な意志を持ってシステムを進化させる方向を選択することと、それを実現する力を持つことの両方を求められる。

ITのさらなる進化に向けて、ナビゲーションとソリューションの両面から顧客企業を支援していくことは、NRIグループの１つの使命であると私たちは考えている。 ■

クラウドサービスをセキュアに利用するには

クラウドコンピューティング（以下、クラウド）はこの１年ほどの間にキーワードとしてすっかり定着し、各種のクラウドサービスも提供されているが、セキュリティ上の懸念から導入に踏み切れない企業も多い。本稿では、法・制度、技術、運用の各観点から、クラウドコンピューティングを安全に利用するために利用者が留意すべき課題について考察する。

利用者が把握しにくいクラウドサービスの実態

企業がクラウドサービスにセキュリティ上の懸念を感じるのは、クラウドサービスが社外のデータセンター上で提供されるため、利用者側でその実態を把握することが困難だからである。セキュリティに関する情報を開示するクラウドサービス事業者もあるが、利用者の側でもクラウドサービスの課題と対策について把握しておく必要があろう。

以下では、NRIセキュアテクノロジーズが2009年度に経済産業省から受託した「クラウドコンピューティングセキュリティ技術研究開発」事業での検討を踏まえ、クラウド環境におけるセキュリティ上の課題について、主に利用者の視点から整理する。

法・制度的観点から見た課題

クラウドサービスに関係の深い法・制度上の課題を整理すると表１のようになる。クラウドサービスは、それが法・制度を遵守するものになっているかどうかを利用者側で判断しにくいという特徴がある。そのため、クラウド事業者側に情報開示を求め、事業者側で対応しきれない部分は利用者側でカバーできるのかなどを判断する必要があろう。

最も大きな課題はデータの保護である。海外の大手クラウド事業者のサービスには、利

表１　法・制度的観点から見た課題

項　目	内　容
データの保護・保全	・サーバー設置国やネットワーク経由国の法令によって情報開示が義務付けられている場合に、データの機密性が守られず情報が強制的に閲覧される可能性がある ・クラウド事業者の事業主体が海外にある場合、海外の準拠法が指定されるケースがある ・営業秘密をクラウドで管理した場合、不正競争防止法の秘密管理性の要件を満たすことができなくなる可能性がある ・犯罪捜査によりクラウド事業者が保有するサーバーが捜査当局に押収された場合、利用者は事業を継続できなくなる
利用者のITガバナンス	・利用者が内部監査を行う場合に、必要な監査証跡をクラウド事業者が提供できない場合がある
データの不正利用の防止	・クラウド環境上に保存されたデータの物理的な所在が明らかでないと、データの不正アクセスがどのサーバーで発生したか特定できない可能性がある ・バックアップなどの目的でデータが複数のサーバーに分散保存されている場合、利用者がデータを削除した時にすべてのデータが削除されないと、データの不正利用や、個人情報保護法違反のリスクが生じる

NRIセキュアテクノロジーズ
事業開発部
セキュリティコンサルタント
篠崎将和（しのざきまさかず）

専門はセキュリティ診断、Webアプリケーションユーザ認証方式設計・開発など

表2　技術的観点から見た課題

項　目	内　容
ネットワーク	・通信路（クラウド事業者内、クラウド事業者間、利用者とクラウド事業者間）の信頼性と通信品質の確保 ・中間者攻撃、なりすまし、サイドチャネル攻撃、リプレイ攻撃などによる通信盗聴（機密性） ・DoS攻撃やDDos攻撃による、自社システムに対する直接的なサービスの妨害、他社システムに対する間接的なパフォーマンスへの影響
サーバー	・マルチテナント環境下での利用者間の情報漏えい（ストレージ、メモリー、ルーティングなどの設定不備、OSやWebアプリケーションサーバーのぜい弱性対策不備）
アプリケーション	・アプリケーションのポータビリティ（移行容易性）（クラウド事業者と自社システム間、クラウド事業者間） ・EDos攻撃によるサービス利用料金の増加
データ	・利用者がデータ削除やサービス解約をした後のデータ復元や情報漏えい ・クラウド事業者によるデータ削除が証明されず利用者が確認できない ・データ保存時の暗号化の必要性、暗号化キー管理の必要性

中間者攻撃：暗号通信を盗聴する手法の1つ
サイドチャネル攻撃：暗号装置の動作を読み取る手法の1つ
リプレイ攻撃：ログイン情報を盗聴し同じデータを使って不正にアクセスする手法
DoS（Denial of Service）攻撃：不正なデータの送信やトラフィックの増大を仕掛けサービスを妨害する手法
DDoS（Distributed DoS）攻撃：多数のコンピュータから特定のサーバーへパケットを送り通信機能を停止させる手法
EDoS攻撃（Economic Denial of Sustainability/Service）：不正アクセスにより膨大な従量課金の料金を発生させる手法

用者が預けたデータをバックアップなどの目的で世界各地の複数のサーバーに分散して保存するものも多い。この場合、利用者がデータを削除した時にはすべてのバックアップデータも削除されないと、データが不正に利用されるおそれや、個人情報保護法を守れないおそれがある。そのため、個人情報や営業秘密などの機密情報をクラウド上に保存する場合には、データの暗号化などの対策を利用者側で行うことも必要となってくる。

また、日本国内のサービスであってもデータは海外のサーバーに保存されるケースも多く、その場合はサーバー設置国やネットワークの経由国の法律に縛られることが考えられる。クラウド事業者が何らかの訴訟に巻き込まれた際は、捜査機関がサーバーを差し押さえる可能性もある。そのため、サービスの準拠法を事前に確認しておく必要がある。海外の大手クラウド事業者の中には、日本の利用者の不安を取り除くために、データセンターをアジア地区に設置したり、日本の法律に準拠することを明示したりするところもある。

技術的観点から見た課題

技術的な観点からの課題は表2のようになる。ネットワークのセキュリティをはじめクラウド事業者側で対応しなければならない課題が多いが、利用者側でリスクを軽減したり、リスクの影響を小さくしたりできるものもある。クラウドサービスは複数の利用者が同じシステムを共有する“マルチテナント”であること、仮想化技術や分散処理技術を利用し

ていることから、同じシステムを企業内に導入した場合と比べてリスク要因が多く、リスクの影響範囲もより大きい。

PaaS（Platform as a Service：OSやミドルウェアの機能をネットワーク上で提供する仕組み）やHaaS（Hardware as a Service：サーバーやストレージなどのハードウェア機能をネットワーク経由で提供する仕組み）を利用する場合、アプリケーションのセキュリティは利用者側で対策を行う必要がある。クラウド事業者がアプリケーションを提供するSaaS（Software as a Service：ソフトウェア機能をインターネット上のサービスとして利用する仕組み）とはこの点が異なる。

サーバーのセキュリティについても、PaaSやHaaSでは利用者側が定常的にシステム監視を行うことにより、セキュリティ上の危険が発生した時は迅速に対応することが可能となる。

特に仮想マシンのセキュリティについては注意が必要である。クラウド環境ではHaaS上で簡単に仮想マシンを複製することができるため、セキュリティのぜい弱な仮想マシンを数多く作ってしまうケースが多い。仮想マシンを最初に作成する際に十分なセキュリティ設定を施した仮想マシンイメージを作成し、複製する仮想マシンにはこのイメージを適用するという作業手順を確立しておくことが重要である。

データのセキュリティについては、転送中と保存時のセキュリティを分けて考える必要がある。転送中のセキュリティはクラウド事業者のネットワークのセキュリティに依存してしまうが、保存時のセキュリティはデータの暗号化などにより利用者側で対応可能である。データを暗号化する際は暗号化キーの管理が最大の課題となる。暗号化キーは利用者が管理するのが最もセキュリティが高いが、利用者側での管理作業が煩雑になる。このためKMIP（Key Management Interoperability Protocol）のような暗号鍵管理プロトコルを用いて暗号化システム間を接続することが解決策の１つとして提案されている。

運用の観点から見た課題

サービスを導入してからの運用上の課題は表３のようになる。

運用段階では、サービスレベルが確保されているか、事業者がどのようなインシデントに対してどのように対応しているかなどを利用者がモニタリングすることが重要である。ITリソースの利用状況も併せて確認し、状況に応じて設定を変更することも必要である。これを適切に行わない場合、利用者は予期しない金銭的負担を強いられることにもなりかねない。

もう１つの課題は、内部統制に係る監査である。クラウドの特性を考慮した監査基準が確立されると利用者としては安心できるのだが、クラウドサービス向けの明確な監査基準

表 3　運用の観点から見た課題

項　目	内　容
サービスの監視	・従量課金の正確さの確保、不正利用の排除 ・適切なログ取得とユーザーへの提供、モニタリング機能の提供
アクセスコントロール（ID管理）	・仮想OSやハイパーバイザ（仮想マシンを実現するソフトウェア）へのアクセスコントロール、ユーザー利用端末の認証 ・自社システムとクラウド環境での統合認証方式
パッチ管理・ぜい弱性管理	・クラウド内（仮想OS、ハイパーバイザ）のセキュリティ対策 ・パッチ管理
インシデントレスポンス	・インシデント発生時の原因究明や解析などに利用するログの取得（利用者が求めるタイミングでログが開示されるか） ・クラウド環境におけるインシデント調査のレスポンスタイム ・利用者側のインシデント調査チームによるクラウド事業者環境への立ち入り調査の実現性
構成管理	・クラウド構成機器の設定ファイルが事業者側で変更された場合の、利用者側でのバージョン判別 ・複数のクラウドサービスを同時に利用した場合の企業内システムの全体把握
監査	・クラウド監査技法の整備（既存の保証型監査との関連性確認など） ・多数の利用者からの監査要求に対応するための監査法人の人材確保

はまだできていない。これについては今後の課題であろう。

準備段階での検討が重要

利用者が求めるサービスレベルを実現するには、契約約款やSLA（サービスレベル契約）などの合意に至る準備段階が重要である。

この段階で、クラウドサービスを利用する範囲の決定、機密情報として扱うデータの特定、セキュリティの実装方式の決定を行う。その上で、クラウド事業者のサービス継続性や運用方式などを考慮して、実現可能性を検証する。サービスの解約時にデータやアプリケーションが削除されたことを証明する方法や、解約時の違約金の有無も確認するとよい。

技術的なセキュリティが保証されない部分は契約約款やSLAの内容をクラウド事業者と詰めておく必要があるが、事業者によっては約款やSLAの変更に応じないケースもあるので、その場合は再度クラウドサービス導入の可否を判断する必要がある。

クラウドサービスのセキュリティをめぐっては、各種業法のセキュリティ基準などとの関係の見直しが実施されつつあるなど、まだ明確な回答が出ていないのが現状である。利用者はこれらの動向を注視しつつ、最適なサービスと利用範囲を見極める必要がある。

クラウド事業者とサービスの利用者がクラウドのセキュリティを評価するためのガイドラインが、2010年４月に米国のCSA（Cloud Security Alliance）から公開されているので、これを参考に検討することをお勧めしたい（http://www.cloudsecurityalliance.org/cm.html）。■

情報資産管理の適正化に向けて
—「SecureCube / Labeling」による機密度の識別・整理—

企業の中に蓄積される情報の量は年々増大しており、情報漏えい対策ソリューションを導入する企業も多い。しかし、どのような機密度を持つファイルがどこにあるのかを適正に管理しなければ、対策の効果は限定的なものにすぎない。本稿では、「SecureCube / Labeling」によるファイルの機密度の可視化を紹介する。

不十分な情報漏えい対策

日本ネットワークセキュリティ協会（JNSA）の集計によると、2009年の上半期に発生した個人情報漏えい事件は764件（想定損害賠償額2,367億円）で、1年間に1,373件が発生した2008年と比べて減っていない。情報セキュリティ製品やソリューションを導入している企業は多いにもかかわらず、なぜ情報漏えいがなくならないのだろうか。

その大きな原因は、情報の管理が社員個人の裁量に任せられ、統一されたルールの策定と、その適正な運用が企業全体でできていないことにあると思われる。

NRIセキュアテクノロジーズ（以下、NRIセキュア）による2009年のアンケート調査では、機密情報の管理に関する「ルールがない」企業と、「ルールはあっても守られていない／運用できていない」企業が全体の7割近くあり、「ルールがあり正しく運用できている」と答えた企業は全体の2割程度にすぎなかった。

筆者の経験からも、情報の機密度が一目でわかるようになっていないという悩みはよく聞かれるところである。また、増え続ける情報資産に対して、その所在を正しく把握できていないケースが多いのも現状である。

機密度の識別と台帳管理の重要性

情報の機密度に関するルールと、その運用の課題は、以下の3点に整理できる。

(1) 情報の種類に応じたルールの策定

一口に重要情報といっても、製品や営業戦略に関わる機密情報や、顧客の個人情報などさまざまな種類のものがある。誰が情報を閲覧してよいかのルールもその種類に応じて決める必要がある。例えば「顧客の個人情報の閲覧は営業担当者および業務上その閲覧が必要な社員に限定する」などである。

「営業情報」に関して注意が必要なのは、2009年に改正された（施行は2010年7月1日）不正競争防止法においては、「営業秘密」を不正に持ち出すだけでも刑事処罰の対象になったことである。同法では、「営業秘密」は以下の3つの要件を満たすものと定義されている。

①秘密管理性

情報にアクセスできる者を制限でき、かつその情報が秘密であると認識できるなど、情報が秘密として管理されていること。

②有用性

客観的に事業活動などに利用されている有

NRIセキュアテクノロジーズ
営業推進部
セキュリティコンサルタント
船越洋明（ふなこしひろあき）

専門はセキュリティ製品やその市場動向、製品マーケティング

用な営業上または技術上の情報であること。

③非公知性

公然と知られておらず、情報保有者の管理下以外では一般に入手できないこと。

このように不正競争防止法の観点から見ても、情報の識別・整理によって機密度を目に見える形にし閲覧対象者を制限することが強く求められる。

(2) 情報の機密度を識別・分類する習慣

ルールを策定し機密度を定義することに加えて、実際に電子ファイルの機密度を目に見えるようにするための手段と、また社員に対して機密度の識別・分類を徹底させるための手段も必要である。

電子ファイルの機密度を誰の目にも分かるようにするためには、紙の書類に「社外秘」などのスタンプを押すのと同様に、ファイルに電子的にスタンプを押す（画面上で文書にスタンプが押された状態にする）方法が一般的である。しかし、スタンプを張り付ける判断や種類の選択など、運用が社員個人の裁量に任せられ、ルールが徹底されていないケースは多い。

こうなると、本来は「秘密」として守られるべき情報が簡単に外部に流出することは避けられない。

(3) 台帳による情報の管理

情報セキュリティ管理に関する必要事項は、ISO/IEC 27001やJIS Q 27001のような標準規格にもまとめられている。これを具体化したISMS（情報セキュリティ管理システム）に基づいてリスクアセスメントを行う場合、「情報資産の洗い出し」を行う必要があり、そのためにはまず管理台帳を作成しなければならない。これにより電子ファイルの所在や作成者、機密度の情報などが整理される。

しかしながら、情報資産は情報共有を目的としたファイルサーバーや、多数の社内のPCに散在する。例えば機密情報のファイルが作成される流れを考えてみると、まず作成途中のファイルが作成者のPCに保存され、内容をチェックするために複数の社員がそのファイルを共有し、完成した電子ファイルがファイルサーバーに保存される。さらにその電子ファイルは、日々の業務によって内容が変更されたりコピーされたりする。このようにして増殖するすべてのファイルの情報をいかにして漏れなく台帳に記録し管理するか、これも大きな課題である。

情報の識別・整理を支援

NRIセキュアでは、以上のような課題を解決するための情報識別・整理ソフト「Secure Cube / Labeling Personal」を無償配布している（http://www.nri-secure.co.jp/service/cube/labeling.html）。

同ソフトをPCにインストールすれば、オフィスで使われることの多いMicrosoft社の「Word」「Excel」「PowerPoint」の各ファイルと、Adobe社のPDFファイルに対して以下

の操作が行えるようになる。

(1) 機密度の可視化とファイル情報への付加

機密度に応じてファイルに「極秘」や「社内限」などのラベルを付与する。これにより、誰が見てもそのファイルの機密度が分かるようになる。

過去、情報漏えいが不正競争防止法に違反するかどうかが争われた訴訟で、当該の情報に「社外秘」などのラベリングが行われていなかったため「営業秘密」であると明確に認識されないとして違反と認定されなかった例がある。ラベルによって「秘密」であることが明示されていればこのようなことは起こらない。ラベルは初期設定の「極秘」「社内限」「関係者限（社内／社外）」「公開情報」のほか、任意に作成することも可能である。ラベル付与は、ポップアップ画面の一覧から「極秘」や「社内限」などをクリックして選択するだけでよい。

視覚的なラベルに加えて、機密度の情報をファイル情報にデータ付加することができ、他のソリューションと連携させて機密度に応じてファイルを操作することが可能になる。例えば、メールフィルタリング製品と連携させて、「極秘」扱いのファイルをメールに添付して送信できないようにすることができる。

このように、ラベルによる機密度の可視化と、機密度をファイル情報として保持することにより、企業が従来から導入しているセキュリティ対策ソリューションがより効果的に機能するようになる。

(2) 行動プロセスへの組み込み

上記の4種類のファイルを作成する際に、機密度のラベルを付与しないとファイルを保存できないように設定し、ラベル付与を義務づけることができる。これによって情報の重要性に対する社員の意識を高めるとともに、ラベルの付与を習慣づけることも可能になる。

Enterprise版による全社管理の実現

「SecureCube / Labeling Personal」はあくまでも各ユーザーのPCに限定した情報管理ツールであるが、これと組み合わせて全社で統合的な情報管理を行える、管理サーバー用の「SecureCube / Labeling Enterprise」（有償）の提供を2010年2月から開始した。

具体的には以下の3つの機能を実現する（図1参照）。

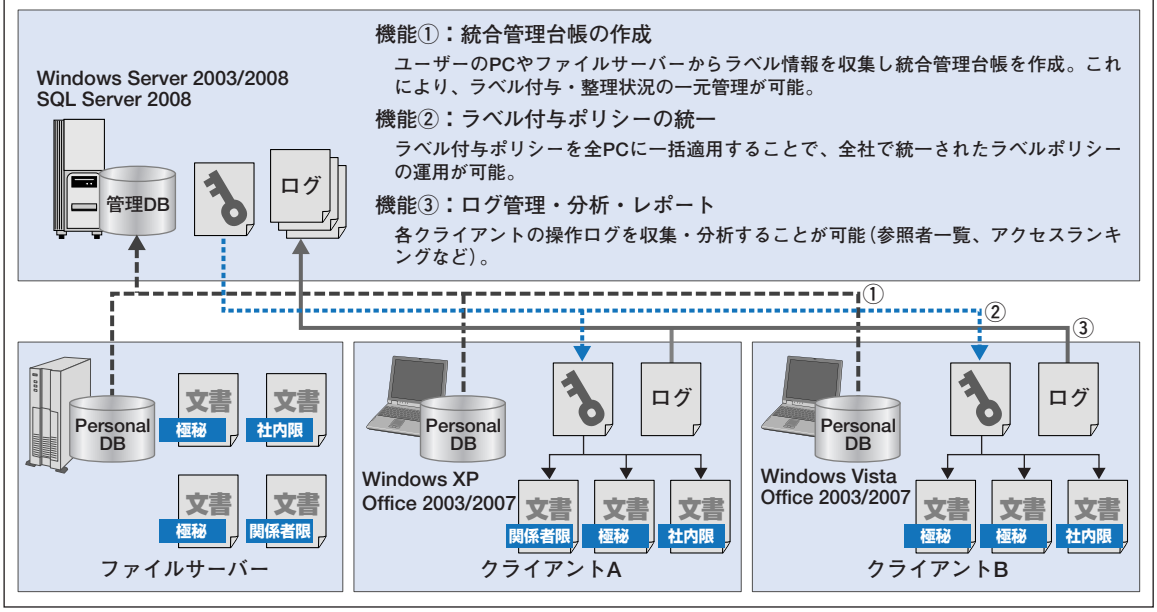
①統合管理台帳の作成

管理対象であるPCやサーバー上のラベル情報を自動的にEnterpriseサーバーに収集し、全社のファイル情報を1つの管理台帳にまとめることができる。管理台帳は、ファイル名、そのファイルが格納されたフォルダ名、ラベルの種類などが記載された「Excel」の表として作られる。これにより、どのような情報が社内のどこに存在するのかを容易に把握できるようになる。

②ラベル付与ポリシーの統一

どのような条件であればどのラベルを付与

図1「SecureCube / Labeling Enterprise」の機能イメージ



するかといったルールを全社ルールとして決めておき、そのルールを全社員に強制的に適用させることができる。これにより、個人の裁量や判断ではなく全社統一のルールに基づいて情報の識別・分類が行えるようになる。

③ログ管理・分析・レポート

ラベルの付与や変更、印刷などの操作を誰が、いつ行ったかというログの収集ができ、情報管理がより徹底される。参照者一覧やアクセスランキングなどの分析も可能である。

以上の機能により、企業内の管理者はファイルの保存場所などの情報を正確かつタイムリーに取得でき、機密情報が本来あるべき場所（ファイルサーバーなど）であるべき姿（適切な機密度）で適正に管理されているかを確認することができる。

企業文化としての情報資産管理のために

NRIセキュアでは、全社員のPCに「Secure Cube / Labeling」がインストールされ、ファイルへのラベル付与が義務づけられている。顧客や社外パートナーに提出するファイルにも「極秘」や「関係者限」のラベルを付与して、社外に対しても当該ファイルの機密度を明示している。このようなルールの統一的な運用は、社外のパートナー企業などと機密性の意識を共有することに役立っている。

「Secure Cube / Labeling」のようなツールを用いた情報識別・整理は、情報管理の1つの手段である。それによって、増大する情報資産を適正に管理する習慣が企業文化として根付いていくことが重要であろう。 ■

メール送信後の情報漏えい対策
―送信先のファイルを保護するソリューション―

社外メールの事前承認や、USBメモリーへのデータ書き出しの禁止など、重要情報の社外への流出を防ぐため各種の対策が行われている。しかし、そのような方法を用いても、社外の相手に渡った後のファイルの情報漏えいは防げない。本稿では、ファイル送信後の送信先における情報漏えい対策を送信元がコントロールするアプローチを紹介する。

添付ファイルのセキュリティ対策

NRIセキュアテクノロジーズ（以下、NRIセキュア）が2009年に実施した「企業における情報セキュリティ実態調査」で、メールのセキュリティ対策について聞いたところ、「添付ファイルの暗号化」「添付ファイルへのパスワード設定」をあげた企業が多かった。しかし、ルールがあってもその適用を社員個人に任せていると、「パスワード設定が面倒」などの理由でルールが十分に守られないケースも多いのではないだろうか。

また、いったんファイルを送ってしまえば、その情報漏えいを防ぐ手段は送信先の対策にに依存する。送ってしまったファイルに対する操作を送信者がコントロールする簡便な手段はなかなかないのが現状である。

“あて先”におけるセキュリティの必要性

NRIセキュアは、安全なファイル送受信環境を実現する「クリプト便」サービスを2001年８月から提供している。Webブラウザーを利用するため操作も簡単で、ファイルおよび送受信経路は暗号化されている。誰が、いつ、どのファイルを送ったかというログを取得でき、不正送信を抑止する効果もある。送信先を間違った場合には、相手がファイルをダウンロードする前であれば送信を取り消すこともできる。しかし、これらの情報漏えい対策でも、ファイルが相手に届くまでのセキュリティしかカバーできない。

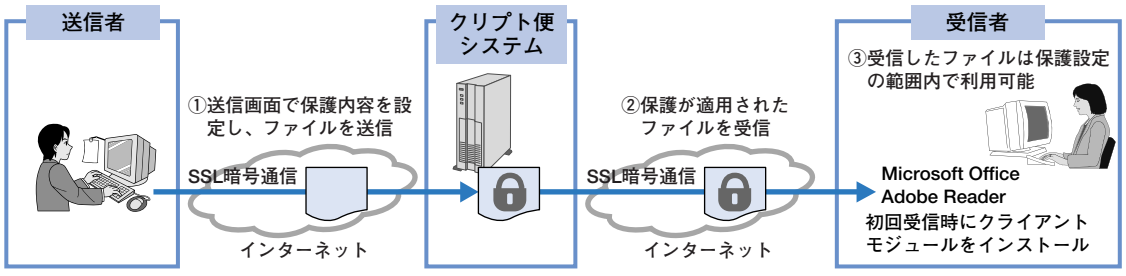
2010年３月に提供を開始した「クリプト便」のファイルコントロールオプション（以下、FCオプション）は“あて先”でのファイルの二次利用や情報漏えいを防ぐ機能を持っている（図１参照）。

FCオプションによって送信されたファイルは、専用プログラムをインストールすることによって開けるようになる。ファイルを開けるのは受信したPCのみで、USBメモリーなどに保存して持ち出しても他のPCでファイルを開くことはできない。編集やコピーが禁止されるほか、印刷や画面キャプチャをできないように設定することも可能なので、紙媒体からの漏えいを防ぐこともできる。

ファイルの保存期間やディスクへの保存可否も設定できる。保存期間を設定しておくと、期間を過ぎてファイルにアクセスした時点でPCから自動的に削除される。ファイル保存を許可しない設定にすれば、ファイルはPC

NRIセキュアテクノロジーズ
ソリューション事業部
セキュリティコンサルタント
田中大介（たなかだいすけ）
専門は情報セキュリティに関する
製品・サービス企画

図1「クリプト便」FCオプションの概要



分類	保護項目	内容
基本的な保護機能（強制的に設定）	ファイルの暗号化	受信したファイルを暗号化して保存。受信したPC以外ではファイルを開くことができない
	編集の禁止	開いたファイルの編集（文字入力など）ができない
	コピー・ペースト操作の禁止	開いたファイルでのコピー・ペースト操作ができない
送信者が任意に設定可能な保護機能	閲覧・保存	ローカルディスクへの保存を許可するか否かを設定可能。また受信後に閲覧可能な日数を設定可能
	連続閲覧	画面表示されたファイルの1回当たりの閲覧可能時間を設定可能
	画面キャプチャ	画面表示されたファイルの画面キャプチャを許可するか否かを設定可能
	印刷	ファイルの印刷を許可するか否かを設定可能
	背景印刷	ファイルの印刷時に背景印字を行うか否かを設定可能

に保存されず、Webブラウザーによってオンラインでのみ閲覧できる。さらに、「クリプト便」の接続IP制限と組み合わせて特定のIPアドレスを持つPCからしかアクセスできないようにすることで、より安全な情報共有が実現できる。

FCオプションが設定できるファイルは、Microsoft社「Word」「Excel」「PowerPoint」のファイルとPDFファイルである。

FCオプションの活用方法

例えば設計事務所の場合は、業者に見積もり資料として図面を提供する際に、ファイルの保存期間を見積提出期限に合わせることや、印刷禁止に設定することにより、相手先での目的外使用を防ぐことができる。

保険会社の場合は、営業員が常に最新の保険料率計算シート（「Excelファイル」）を使用するようにするために、保険料率の有効期限と「Excel」ファイルの閲覧期間を合わせるといった使い方が想定される。こうすれば、営業員が最新でない計算シートで保険料率を計算するという事態を防げるだろう。

情報漏えい対策は、自社だけの対策では不十分である。送信先における情報の保護までを考慮してはじめて有効な対策となる。 ■

社内文書の効率的で安全な共有のために
―ファイルサーバー統合管理ソリューション―

企業内のビジネス文書が加速度的に増え、文書共有・管理のためのファイルサーバーの数も増え続けている。問題は、それによって文書管理が複雑化し、セキュリティの不備が生じていることである。本稿では、現状の文書管理の問題点を整理するとともに、野村総合研究所（以下、NRI）の「File Server Protector」による統合管理手法を紹介する。

ファイルサーバー利用上の課題

企業内で情報を管理・共有する手段として、簡単に設置できて使い方も簡単であることから、多くの企業でファイルサーバーが使用されている。しかし、ファイルサーバーが乱立したために管理負荷の増大や情報漏えい対策の不備を招いているケースも多い。

ファイルサーバーは、社員間やパートナー企業との間で情報を共有するための効率的な手段だが、それは情報漏えいや改ざんのリスクと表裏一体である。

ファイルサーバーの運用において、システム管理者はフォルダーの整理やアクセス権の管理などに細心の注意を払う必要がある。こうした管理がおろそかになれば、ファイルサーバーの統制が崩れ、情報漏えいのリスクを抱えることになる。

ハードルが高い文書管理システムの導入

このような問題の解決策の１つは文書管理システムの導入である。しかし、本格的な文書管理システムの導入は一般的にはハードルが高い。

まず文書管理システムの導入に当たっては、文書情報の棚卸し（既存文書の管理方法やライフサイクルなど）と、文書が保管されているインフラ情報の調査を実施する必要がある。その上で、現行システム（ファイルサーバーなど）の存続可否や、移行対象文書の精査など、文書管理システムに移行する範囲の特定を行う。このほか文書管理システム導入後の運用ポリシーや運用手順の策定、業務プロセスの変更も必要になる。さらにシステムの運用コストも考慮しなくてはならない。

ファイルサーバーという極めて簡便なインフラが乱立しているために、文書管理システムの導入には多くのコストがかかるのが現状である。

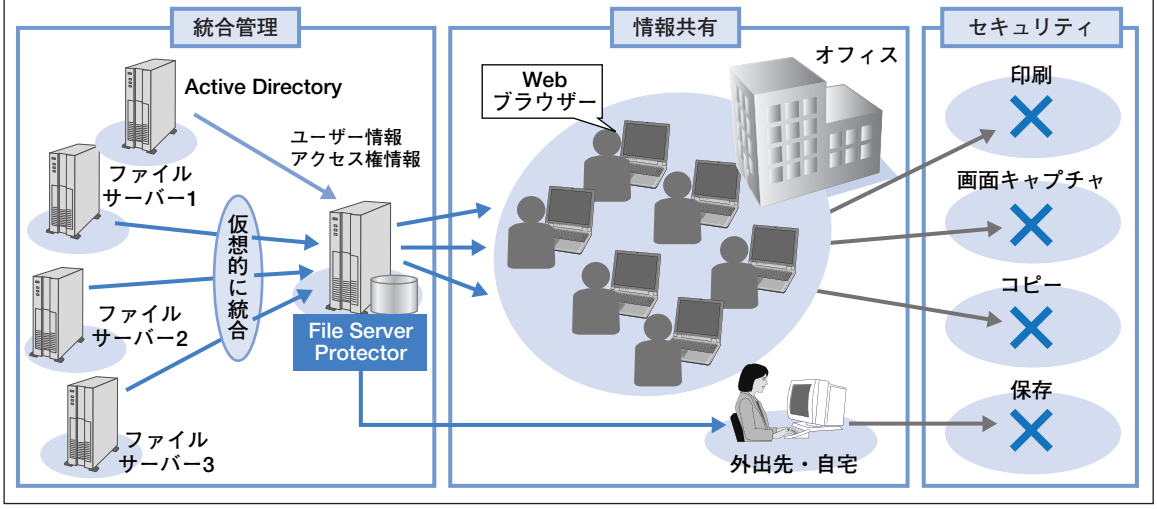
管理コスト削減とセキュリティ強化を両立

上記の問題点を解決するのが、NRIのファイルサーバー統合管理ソリューション「File Server Protector」である（図１参照）。

「File Server Protector」は、ファイルサーバーとユーザーとの間に管理サーバーを配置するだけのシンプルな構成で、既存文書を移行することなく、従来のファイルサーバー環境をそのまま利用することができる。またMicrosoft社のActive Directory（ドメイン管

野村総合研究所
基盤ソリューション事業本部
DIソリューション事業部
副主任システムコンサルタント
兼子和巳（かねこかずみ）
専門はコンテンツ管理における企画・開発

図1「File Server Protector」の導入イメージ



理のためのディレクトリサービス）と連携してユーザー情報やアクセス権情報を引き継ぐことができるため、運用手順や業務プロセスの変更を最小限に抑えられる。主な機能は以下のとおりである。

①統合管理

複数のファイルサーバーがあっても、そらは仮想的に統合され、従来は分散管理されていた文書を1つの画面上から参照・管理できるようになる。

②情報共有

Webブラウザーを利用する方式のため、社内のイントラネットだけでなく外出先や自宅からでもインターネットを通じてファイルサーバーにアクセスすることができ、文書の共有が格段に容易になる。

③セキュリティ

「File Server Protector」を使用して閲覧された文書は、持ち出しや二次利用を制限する以下のようなセキュリティの設定が可能である。

・保存制御：ユーザーのPCへの保存の可否
・印刷制御：印刷の可否
・キャプチャ制御：画面キャプチャの可否
・編集制御：加筆や訂正、コピー&ペーストなど文書変更の可否

このように、「File Server Protector」は、前述の文書管理システム導入のハードルを回避しつつ、簡便に既存ファイルサーバーの統制を可能とする。

内部統制の強化が叫ばれ、同時に既存資産を無駄にせずIT投資の効果を高めることが求められている昨今、スピーディーかつ簡便な方法により効率的で安全な文書共有を実現する「File Server Protector」の有用性は高いと思われる。 ■

IT投資管理のグローバルスタンダード
―改訂された「Val ITフレームワーク」―

2008年７月に発行された「Val IT Framework」（以下、「Val IT」）第２版の日本語版が2010年２月に公開された。「Val IT」は、IT投資から価値を引き出すために必要な管理施策を、経営者の観点から包括的かつ体系的にまとめたフレームワークである。本稿では、「Val IT」の概要と改訂のポイントを紹介するとともに、「Val IT」を実務でどう活用していくか提案する。

３つのドメインでIT投資を管理

米国のITガバナンス協会（ITGI）による「Val IT」は、2006年に初版が発行された。IT投資により価値を生み出すためには、ITのみならずビジネスの領域にまで管理を広げる必要がある。ITを有効活用して企業価値を高めるといった、経営戦略やコーポレートガバナンスの領域に踏み込んだ、他に類を見ない包括的なフレームワークが「Val IT」である。「Val IT」は、「価値ガバナンス」「ポートフォリオ管理」「投資管理」という３つのドメイン（領域）に分けて、具体的なプラクティス（管理施策）や評価項目などについて詳述している。以下、各ドメインの内容を簡単に紹介する。

(1) 価値ガバナンス

価値ガバナンスは「Val IT」の土台となるドメインである。IT投資から確実に価値を引き出すためには、まず企業内の組織の役割と権限・責任を明確化すること、すなわちガバナンス設計が必要である。その際には、取締役会、CEO（最高経営責任者）、CFO（最高財務責任者）、CIO（最高情報責任者）などに加えて、経営層の意思決定を補佐する「投資サービス委員会」や、事業部門やIT部門を支援する「バリューマネジメントオフィス」など、IT投資から価値を最大限に引き出すために必要な支援組織についても役割や責任を明確にする必要がある。

(2) ポートフォリオ管理

ポートフォリオ管理では、数あるIT投資案件の候補群から、経営資源（特に人的資源）の制約のもとで、価値を最大化するための案件の最適な組み合わせ選択を行う。案件の選択の際には、期待効果の大きさのみならず、効果が得られないリスクの大きさにも着目しなければならない。効果とリスクのバランスを考慮して、偏った投資が行われることのないよう注意すべきである。

(3) 投資管理

投資管理ドメインでは、IT投資のアイデアが生まれてから投資案件として具体化し、投資を実施してシステムを稼働させ、実際に価値が得られるまでの一連の工程で必要なプラクティスがまとめられている。いまやIT投資は、IT単独ではなく事業戦略や業務改革などIT以外の取り組みと一体となることによって価値が最大化される性質のものが増えている。そのため、ITとIT以外の取り組みを「プログ

野村総合研究所
システムコンサルティング事業本部
プロセス・ITマネジメント研究室
上級コンサルタント（公認会計士、CGEIT、CISA）
下野谷　益（しものやみつる）
専門はITサービスの管理会計

ラム」という１つの概念でとらえ、工程の節目ごとに前に進むか中止するかを判断する仕組みを整備すべきである。

改訂のポイント

「Val IT」は2008年７月に第２版に改訂された。改訂のポイントは、プラクティスの見直しや拡充もさることながら、ITガバナンスのフレームワークであるCOBITと同様に、ドメイン、マネジメントガイドライン、成熟度モデルといった構成に改めた点にある。これによってページ数が約３倍（日本語版で118ページ）に増えるとともに、質的にもフレームワークとしての充実度が増した。改訂の背景には、先行するCOBITと体裁をそろえることで、将来この２つのフレームワークを統合する道筋をつける意図があったと考えられる。

改訂によりプラクティスが40から69に増加・再編され、COBITと同様の構造を持つマネジメントガイドラインが新たに導入された。「Val IT」の初版は、プラクティスとして提示されたものの中に、具体的な行動ではなく、あるべき状態の目標が混在していることが難点の１つにあげられていた。そのため、プラクティスについての記述を読んでも、あるべき状態に至るまでに誰が何をすればよいのか、最終目標にたどり着くまでの中間目標は何かなど、直ちに理解しにくいところがあった。マネジメントガイドラインによってプラクティスの中身が整理されたことで、こうした難点が解消され、フレームワークの理解も容易になったといえる。

マネジメントガイドラインは、プロセスごとに必要なアクティビティをまとめ、誰がどのアクティビティに関して実行責任・説明責任を負うのかを詳細に示したものである。併せて、それぞれの役割の定義および役割の相互関係がモデルとして示されている。

このほか、COBITと同様に、各ドメインごとに６段階の成熟度モデルが導入され、IT投資管理の成熟度を測る目安が示された。

なお、野村総合研究所（NRI）が翻訳を担当した「Val IT」第２版の日本語訳は、日本ITガバナンス協会のサイトからダウンロードできる（http://www.itgi.jp/download.html）。

「Val IT」をどう使うか

「Val IT」で示されたプラクティスをすべて行っている企業は、世界でもまだ少ないであろう。当面は、新たに導入されたマネジメントガイドラインと成熟度モデルを、自社のIT投資管理の現状を診断するツールとして活用するだけでも有用と考えられる。この診断によって自社のIT投資管理の水準や、不足しているプラクティスなどを知ることができる。簡易に自己診断するのであれば、成熟度モデルのみを利用してもよい。このようにして成熟度レベルの測定データが蓄積されていけば、「Val IT」は名実ともにIT投資管理のグローバルスタンダードとなるだろう。 ■

米国で注目されるクラウドブローカーの動向

米国を中心にクラウドコンピューティング（以下、クラウド）をめぐる動きがますます活発になってきている。注目すべきものに、大手ベンダーのクラウドサービスをユーザーに仲介するクラウドブローカーの出現がある。本稿では、クラウドブローカーのサービスの概要を紹介し、エンタープライズクラウド市場の今後の動向について展望する。

拡大するクラウドサービス

米国でクラウドに対する関心がますます高まっている。

Microsoft社は2008年に発表した「Windows Azure」（アプリケーションとデータをホスティングするクラウドプラットフォームサービス）を2010年１月から正式に開始した。また、Google社はクラウド上のWebアプリケーション開発・実行環境「Google App Engine」の機能拡張を続けている。

いち早くクラウドサービスを開始したAmazon社も次々に新しいサービスを投入している。また、クラウド環境を実現する仮想化ソフトウェア「vSphere」で知られるVMware社も、2009年11月にCisco Systems社およびEMC社との間でVCE（Virtual Computing Environment）連合という名の提携を行っており、その存在感をますます強めている。

クラウドブローカーの出現

クラウドがますます拡大し、大手ベンダー間の競争も激しくなっているなかで、最近よく聞かれるようになってきたのが「クラウドブローカー」という言葉である。これは既存のクラウドサービスを利用してユーザーに新たなサービスを提供する企業のことである。

米国の調査・コンサルティング会社であるGartner社は2009年７月のプレスリリースの中で、これから出現してくると思われるものも含めクラウドブローカーには以下の３つの種類があるとしている（http://www.gartner.com/it/page.jsp?id=1064712）。

①Intermediation（仲介）

大手クラウドベンダーのサービスにブローカーが付加価値を付けてサービスを提供する。

②Aggregation（統合）

複数のクラウドサービス間のデータ統合やサービス統合をブローカーが行う。

③Arbitrage（調停）

複数のクラウドサービスをブローカーが組み合わせて連携させる。

AggregationとArbitrageとの違いは、Aggregationはクラウドブローカーが指定する特定のクラウドサービスの利用を前提とするが、Arbitrageはユーザーが柔軟にクラウドサービスを選択できる点にある。

クラウドブローカーの実例

データセンターに関連した情報を発信して

NRIアメリカ
主任テクニカルエンジニア
相田洋志（あいだひろし）
専門は基盤技術のリサーチ・検証

いるサイト「Data Center Knowledge」は、記事の中で13のクラウドブローカーを列挙している（http://www.datacenterknowledge.com/archives/2010/01/22/cloud-computing-brokers-a-resource-guide/）。この中からいくつかを紹介しよう。

RightScale社、Elastra社のサービスは、リソース管理や仮想マシンイメージ管理など、管理に特化した機能を提供する。Amazon社などが提供するクラウドサービスのリソースを利用しつつ、より高度な管理機能を望むユーザーを対象としている。上記の分類では①の仲介型に入るが、VMware社などのクラウドサービスへの対応も進めてきており、②の統合型と③の調停型の機能も持っている。

Deltacloudは、統合型や調停型のクラウドブローカーサービスをAPI（アプリケーションで使用する命令・関数を定めた規約）によって実現しようとするプロジェクトである。例えばAmazon社とVMware社ではクラウドサービスを操作するためのAPIが異なるため、通常は同じ操作方法を用いて利用することはできない。Deltacloudはその差分を吸収するAPIを開発しており、実現すれば異なるクラウドベンダーのサービスを同一の操作方法で利用できるようになる。

同様にAPIによるアプローチをとるものに、Eucalyptus Systems社の「Eucalyptus」がある。「Eucalyptus」はプライベートクラウド（企業が自社の基盤上で構築するクラウド環境）を構築するオープンソースの製品で、そのAPIはAmazon社のクラウドサービスと互換性がある。

ユーザーは必要なサービスの見極めを

「Data Center Knowledge」は別の記事で「大手ベンダーがその提供機能の範囲を拡大し、クラウドブローカーがカバーしようとしている機能を独自に提供しはじめる可能性がある」と書いている。すでにAmazon社は管理機能を強化するいくつかのサービスを2009年に開始した。また、これまではパブリッククラウド（広く一般利用者を対象としたクラウドサービス）のみを提供してきたが、セキュリティを強化して企業内環境との連携を可能とするバーチャルプライベートクラウドの提供も開始した。Microsoft社やVMware社も同様に、管理機能の強化、企業内環境とパブリッククラウドとの連携という方向性を持つ製品をリリースしている。

これら大手ベンダーの動向の一方で、クラウドブローカーもそのすき間を縫って、ユニークなサービスでエンタープライズクラウド市場にビジネスチャンスを見出してくることが予想される。

こうした状況のなかでユーザー企業に求められるのは、どのようなタイプのクラウドサービスを必要としているのかを、既存のシステムやリソース、要求仕様に照らして見極めることであろう。 ■

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
コンサルティング事業本部サイト（異才融合）	http://www.consul.nri.co.jp	コンサルティング事業本部の概要や提供サービス、NRIで活躍中の経営コンサルタントの素顔などを紹介
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

2010年 7 月号　Vol.27 No.7（通巻319号）
2010年 6 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