総論：クラウド時代のセキュリティ対策

クラウド環境の脆弱性とセキュリティ対策

―コンサルから実施、監査・改善までトータルソリューションを提供―

さらなる発展が期待される一方で、解決しなければならない重要課題としてセキュリティがあげられるクラウドコンピューティング。セキュリティコンサルから対策の実施、監査・改善まで、クラウド環境に求められるセキュリティ対策のトータルソリューションを提供する伊藤忠テクノソリューションズ（以下、CTC）の取組みを紹介する。

クラウド環境（仮想化環境）のセキュリティ対策が不可欠に

新しいコンピューティングスタイルとしてのクラウドコンピューティングが脚光を浴びる一方で、クラウド環境のセキュリティに対する不安や懸念を抱いている利用者は多い。クラウドコンピューティングが本格的に次世代の基盤テクノロジーとして普及するためには、セキュリティの確保という最重要課題を解決することが必要だ。特にクラウド事業者にとっては、技術的な各種ソリューションを組み合わせながらセキュリティを担保する仕組みを実装するとともに、認証制度（ISMS、SAS-70、PCIDSSなど）やコンプライアンス（個人情報保護法・不正競争防止法等）、情報セキュリティ監査制度への対応状況をクラウド利用者に知らしめることが重要となる。

クラウド環境すなわち仮想化環境のセキュリティに関する影響範囲について、CTCのITエンジニアリング室ミドルウェア技術部部長補佐でセキュリティ技術課長を兼務する伊藤英二氏は、「例えば、サービス不能攻撃（DOS）を受けた場合、これまでは攻撃を受けた物理サーバ(もしくはアプリケーション)がサービス不能に陥るだけでしたが、1つの物理サーバ上で複数のOSが稼動する仮想化ソフトを利用する環境では、仮想化ソフト上で動くすべてのOSとアプリケーションがサービス不能に陥ってしまう可能性があり、攻撃の影響範囲は極めて大きくなります。また、内部からの不正行為に対しても同様のことが言えます。この課題を解決するためには、仮想化環境をセキュアに構築・維持・管理するためのノウハウやメソッドが必要です」と警鐘を鳴らす。

伊藤忠テクノソリューションズ㈱
ITエンジニアリング室　ミドルウェア技術部
部長補佐　**伊藤 英二**氏

仮想化環境には特有の脅威が

仮想化環境の課題として、仮想化

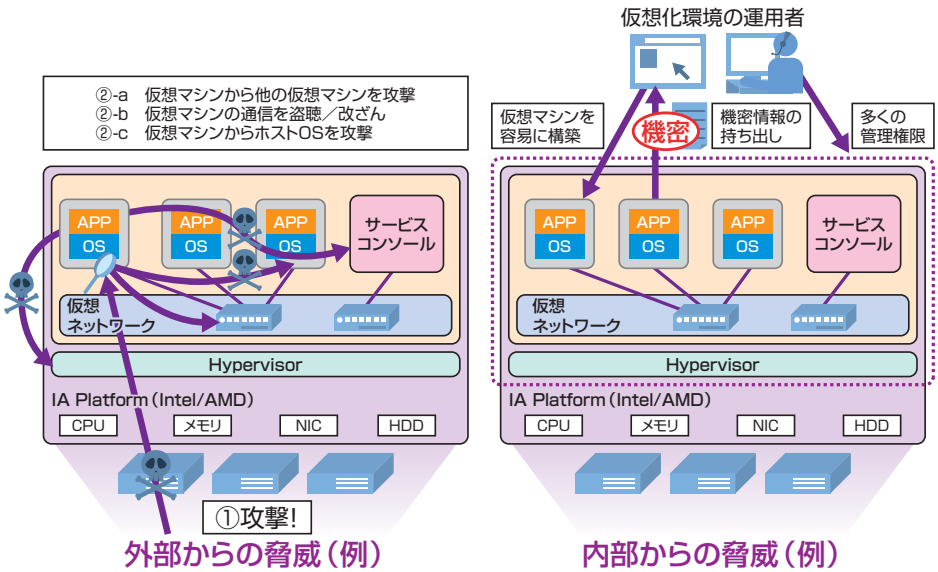


図1　仮想化環境固有の課題

環境特有の脅威があげられる。図1に仮想化環境特有の課題（脅威の例）を示す。外部からの脅威としては、仮想マシンを攻撃後、他の仮想マシンやホストOS（ハイパーバイザー）を攻撃する脅威や、仮想スイッチからの通信盗聴といった脅威があげられる。攻撃された仮想マシンから他の仮想マシン等に対する攻撃の連鎖を防御するためには、仮想マシン間通信制御の仕組みが必要であり、ネットワークも仮想化される仮想化環境では、これまでの物理型の各種セキュリティ対策製品では攻撃を防御することが困難だ。また、仮想マシンに組み込まれるデバイスドライバに含まれる脆弱性への対応、ホストOSの設定の不備を突いた攻撃に対する対策も必要になる。

一方、内部からの脅威としては、仮想化環境によって容易に仮想マシンや、スイッチを増設できるため、システムの構成変更によるセキュリティホールができる可能性が増える。また仮想化環境の管理ツールでは、仮想化環境の運用者が多くの管理権限も持つことができ、設定次第では機密情報の持ち出しも容易に行えるようになる。

仮想化基盤を守りつつ運用を保つセキュリティ対策を提供

以上のような仮想化環境特有の課題を解決するためのセキュリティ対策の方向性としてCTCでは、「仮想化環境とその上で動くサービスを保護するための技術と、運用管理時に求められるセキュリティ要件を仮想化環境（＋その上のサービス）に対応させることの2つを基軸に考えています。」（伊藤氏）

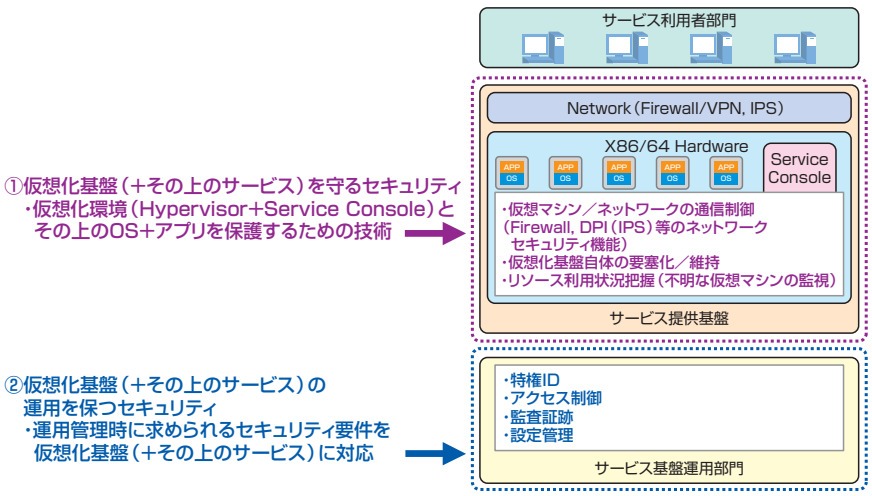


図2　CTCが考える仮想化環境のセキュリティ

CTCでは、企業がクラウド環境を容易に構築可能にするソリューションセット「VM Pool（ヴイエム・プール）」シリーズのラインナップに、この考えに基づくセキュリティ対策のベストプラクティスとして、トレンドマイクロの「Trend Micro Deep Security」（以下Deep Security）と、米Splunk社のITデータサーチエンジン「Splunk」を追加している。

詳細は後続の頁で紹介するが、Deep Securityはファイアウォール、IDS/IPS、Webアプリケーションプロテクション、改竄検知、セキュリティログ監視といった5つの機能を有しており、これらの機能によりクラウド基盤上で動作するOSやミドルウェア、Webアプリケーションの保護を実現する。また、VMware社のVMsafe API を利用した「Deep Security Virtual Appliance」による仮想化基盤の保護も可能にしている。

一方、Splunkは、クラウド基盤の運用面では、特権ID管理、監査証跡など様々なセキュリティ事項の検討に必要なログ管理ソリューションで、シンプルかつ高速な検索機能と豊富なデータ収集方式で簡単かつ効率的に統合ログ管理が実現できるという特長を持つ。Splunkにより、ITインフラにおける様々なデータを集中管理し、リアルタイムに検索・解析を行うことが可能だ。仮想化基盤やその上で動作するOSやアプリケーション、さらにはDeep Security の設定情報やログをSplunkで集約し、検索・分析を行える。

VM Poolシリーズは、CTC独自のプライベートクラウドソリューションだ。様々なベンダーのサーバ、ストレージ、仮想化ミドルウェアを組み合わせ、あらかじめ最適なシステムとして検証済みであるため、プライベートクラウド環境を短期間で

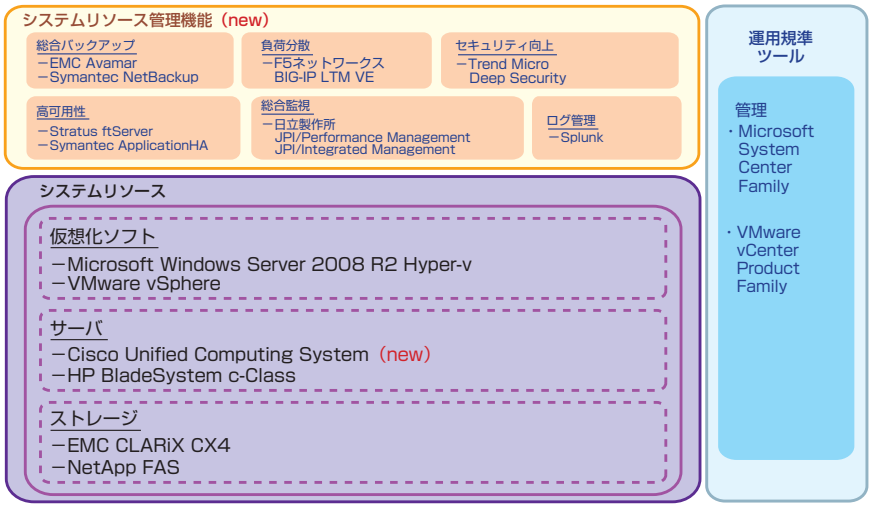


図３　VM Poolシリーズのシステム構成ラインナップ

構築することが可能という特長を持ち、2007年12月より販売を開始してから100件を超える豊富な実績を持っている。

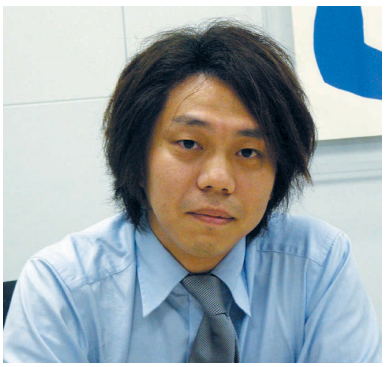
VM Poolシリーズの最新版では、プラットフォームラインナップに米シスコシステムズの「Cisco Unified Computing System」を追加したほか、リソース管理機能として、プライベートクラウド環境における複雑なシステム運用を補完するバックアップやリソース監視といった管理機能及び、仮想化環境に対応したサーバ負荷分散と前述のセキュリティ機能を追加し、プライベートクラウド環境の実現に必要となる要件を満たす機能を総合的にソリューション化している（図３）。

CTCでは今後、プライベートクラウド環境の運用を容易にする自動化機能を拡充するなど、VM Poolシリーズのさらなる機能強化をすることで、プライベートクラウドビジネスの一層の強化を図る方針である。

クラウドコンピューティングの管理基準の策定を支援

CTCでは、プライベートクラウド実現の構想立案を行うコンサルティングサービス「SOIDEAL」や複雑なプライベートクラウド環境における運用課題を解決する「リモート運用サービスRePlavail」等を提供しているが、最近注力しているのが監査の仕組みなど、クラウドコンピューティングの管理基準の策定を支援するサービスだ。

CTCが構築するシステムの「運用」と「セキュリティ」におけるITライフサイクルの各フェーズを支援するITサービスコンサルティング部の佐藤元彦セキュリティアシュアランス課長は、「クラウドコンピューティングに関しては、数々の有用性と対比するように、数々のリスクがあるといわれています。リスクと有用性とを比較して、受容し得るリスクか、もしくは管理策を用いて許容できるレベルにできるリスクかを判断することが重要です」と前置きしたうえで、「クラウドコンピューティングでは、利用者が“管理できない”部分が、SaaS、PaaS、IaaSのどの提供モデルでも発生します。ただし、その管理責任は、委譲できるものではないことから、クラウドコンピューティングに対する懸念（不安）が増幅されていると私は考えています。したがって、クラウドコンピューティングを利用者が責任を持って使うためには第一に、資産分類とリスク分析を行い、預けても良い資産／プロセスを投入することが重要です」と語る。佐藤課長は、日本セキュリティ監査協会のクラウドに関するセキュリティ監査WGリーダ、経済産業省 のクラウドセキュリティ管理基準策定タスクフォース委員を務める情報セキュリティ監査及び情報セキュリティマネジメントのプロフェッショナルだ。



伊藤忠テクノソリューションズ㈱
ITサービスコンサルティング部
セキュリティアシュアランス課
課長　佐藤 元彦氏

日本におけるクラウドコンピューティングのリスクへの対応状況について、佐藤課長は、「現在、私も委

員を務める経済産業省の“クラウドセキュリティ管理基準策定タスクフォース”において、ISO/IEC27001, 27002の観点から利用者視点でクラウドコンピューティング利用のためのリスクと管理策を洗い出しています。この検討を基に、各管理策を実施するための、クラウド利用者による実施の手引、クラウド事業者による実施の手引、さらにクラウド固有の考慮事項を掲載した情報セキュリティガイドラインを作成しています。このガイドラインは、近々パブリックコメントに付されることとなっています」と述べている。

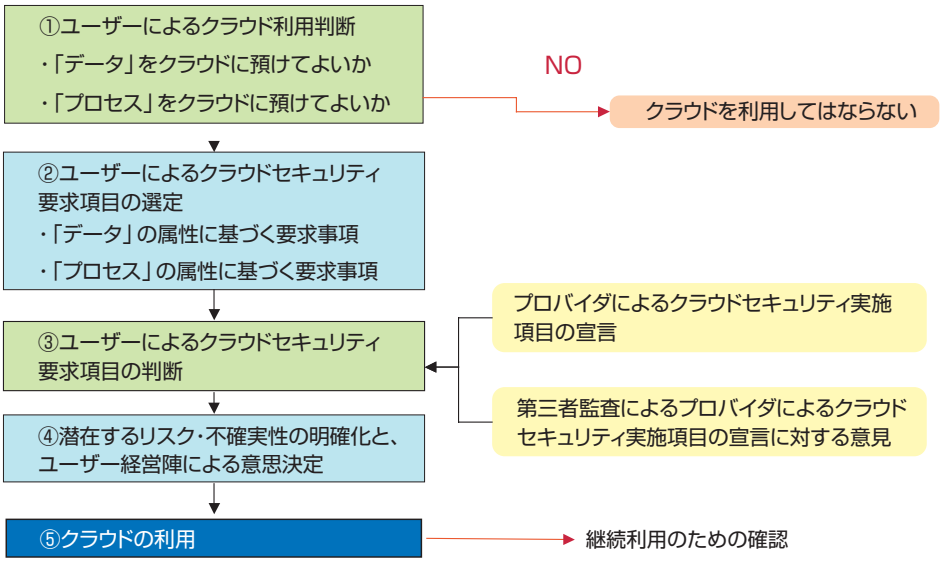


図4　正しいクラウドコンピューティングの使い方を支援

クラウドセキュリティ管理基準への対応によって、クラウド利用者は、クラウドコンピューティングを自らの業務に組み入れるための留意点について、クラウド事業者に確認をすることが可能になる。一方、クラウド事業者は、クラウド利用者が利用をする際のリスク判断に有益となる情報を提供することができ、利用を促進できるといったメリットがある。

佐藤課長は、「管理基準を確認するだけでなく、クラウド利用者は、さらに一歩進み、“Trust, but Verify”の観点で、監査人が監査可能な（証跡が確保できる）仕組みを作ることが重要になります。Verifyの部分がなければ、Trust and Believeとなってしまいます。監査は、この検証を行います。クラウドセキュリティ管理基準が策定された後、それらの事項を確認するための監査手続の導入が重要です」と指摘する。

監査手続は、事業者への監査では、「クラウド事業者が公表・明示すべき情報を準備しているか」という点と、「クラウド事業者がクラウド特有のリスクを認識し、必要な管理策を講じているか」という点を、またクラウド利用者への監査では、「クラウドコンピューティングを利用するにあたって発生するリスクを認識し、必要に応じて管理策を講じているか」を確認する必要があるとしている。

データの保管場所に起因する特殊なリスクのアドバイスも

クラウドコンピューティングでは、データの保管場所に起因する特殊なリスクがある。1つはプライバシーに係わる問題である。特に、欧州域の法人で取得した個人情報を、欧州域以外に移す際に問題になることがある。さらに、従業員の情報であっても、健康診断の結果などは、センシティブな情報に区分される情報が含まれる可能性があり、取扱いに注意が必要となる可能性もある。もう1つは、捜査権に係る問題である。各国では、自国内のデータに関する捜査権や押収権を法的に定義している場合が多く、それらの仕組みが問題にされることもあるが、逆に、海外に設置されたデータには捜査権や押収権が及ばず、犯罪に巻き込まれた場合に海外のデータを保全してもらえない可能性も考えられる。

「CTCでは、こういった特殊なリスクに関するアドバイスを含め、図4に示すようにクラウドコンピューティングを正しく、安心して使っていただけるようなサービスをクラウド利用者・クラウド事業者に提供していきたいと考えています。」（佐藤課長）