アンラボ・セキュリティレター

Press Ahn

2014.6　Vol.06

「数字」で読み解くクラウドの世界

クラウドコンピューターとは

「数字」で読み解くクラウドの世界

2000 年代後半に入り、IT 業界にはクラウドコンピューター (Cloud Computing) という画期的な概念が登場した。一部ではクラウドコンピューターを IT 革命ではなく「Life 革命」とまで表現し、本概念が広まってからは世界的なリサーチグループで発表する IT 動向報告書の恒例テーマとしてピックアップされ、現在も変わらず注目され続けている。クラウドコンピューターは IT 業界の者なら誰もが耳にしているはずだが、きちんと把握することはそう簡単ではない。今回 PressAhn では、クラウドの概念と特徴について詳細に紹介した。

ホテルと一戸建て、どちらが良いか?

妙な質問ではある。ホテルか一戸建てか、短期間の滞在ならホテル、長期間なら一戸建てを選ぶのは当然のことであろう。一戸建てのメリットはマイホームという安心感とプライバシーが保証される点が挙げられるが、電気代や水道代などの各種管理費がかかる上に掃除や修理、強盗対策なども直接当たらなくてはならない。

ホテルは毎日の掃除やシーツの取り替えもホテル側のサービスに任せ、宿泊代さえ払えば電気や水も気兼ねなく使用できる。デメリットはいくらサービスが良くてもマイホームではないため、多くの人が利用しほとんどの器物は私有物ではなく、従業員が掃除と点検のために出入りすることもある。

このような特徴を前提に一つの状況を想定して見よう。

もしあなたの所に数十人の客人が急に尋ねて来て何日か滞在していくことがたびたび発生するとしたら、どのような住居を選んだほうが良いだろうか (極端な例を避けるため一戸建ては 5 人家族が住む 4LDK ほどの広さに設定)。この場合はホテルを考慮する可能性が高くなる。

IT (Information Technology) システムにも、このホテルのようなサービスがある。費用さえ出せばサーバー、ストレージ、ネットワークさえもいくらでも追加できる。ソフトウェア開発に必要なフレームワークのレンタルや、開発するまでもなく必要なハイクオリティのソフトウェアをすぐに入手することもできる。だがユーザーはお金でサービスを利用する以上に、サービスシステムの内部構造を知ることはできない。カラクリは隠されて目に見えないが、スムーズに作業をサポートしてくれるハイクオリティのコンピューターサービス、これを「クラウド(Cloud)」と言う。

クラウドがホテルなら、企業が自主的に運営する IT システムは一戸建てに例えられる。一人一部屋の一戸建てのように、企業の IT システムを構成するサービスも特定のサーバーを所有して使用したりする。Web サービスの場合は Web サーバーで、DB サービスは独自の DB サーバーで運営するのが一般的で、一戸建てのように一部屋ずつ運営しても特に問題はない。だが、ある日トラフィックという客が急に押し寄せてきたらどうだろう。

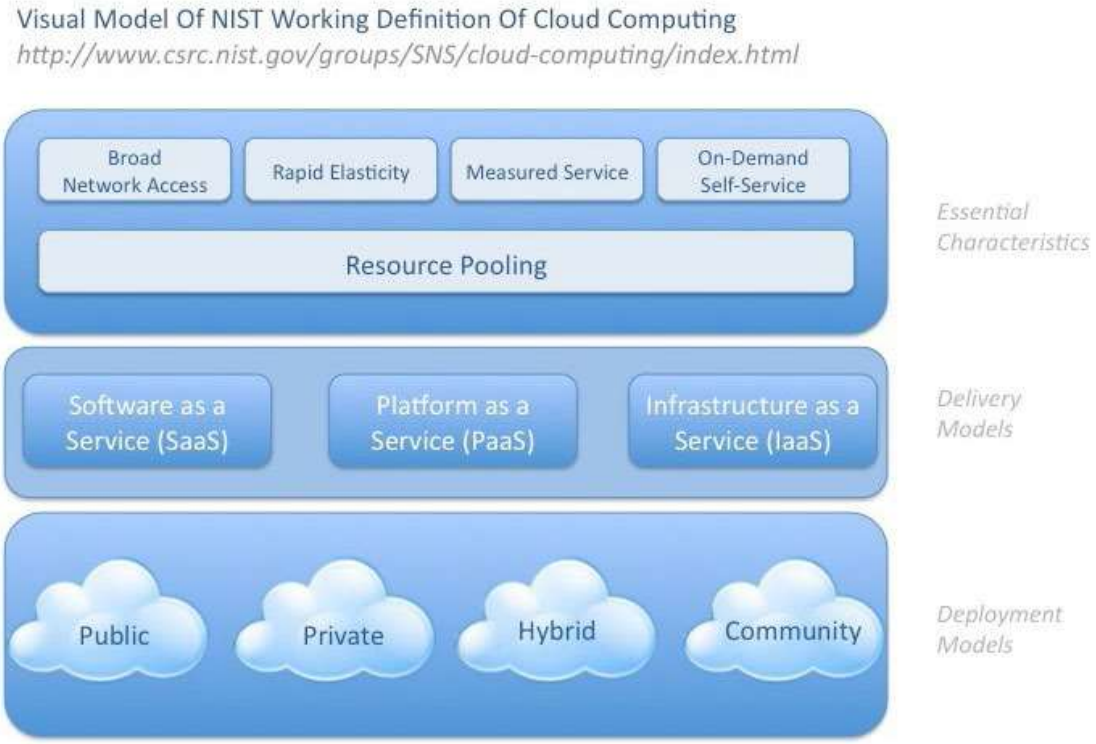
オンラインショッピングモールでは正月に通常の何倍ものトラフィックが集中し、アンラボをはじめとするセキュリティ会社はインシデントが発生するとトラフィックが爆発的に増えたりする。客が押し寄せたら部屋を増やせばいいだけのことだが、短時間で増築するのは簡単ではない。

企業の IT システムも同じで、トラフィックの増加と同時にすぐサーバーを増設するのは難しい。しかもトラフィック増加は一時的なもので数日で収まることなので、そのためだけに通常の何倍ものサーバーを導入するなら予算の問題もある。こんな状況ではやはりホテルのようなクラウドサービスが良い解決策になる。一時的な訪問客のため短期間必要なだけ部屋を借りて費用を払えば良いからだ。

企業側で運営されていたかつての IT システムと異なり、現在の IT 環境は非常に複雑になった。サービスタイプも多様でトラフィック変化も予測がつかない場合が多い。利便性の面から見れば直接所有して運営・管理したほうが勝手が効くが、複雑な IT 環境と急激な変化に対して迅速で柔軟な対応を可能にする面ではクラウドシステムの方が有効である。このような状況を背景に、世界的な IT リサーチ機関・ガートナー (Gartner) の年例 IT 動向予測レポートなど各種の IT 動向報告書ではクラウドは恒例のテーマになっている。ではクラウドの主要概念についてもう少し掘り下げてみよう。

クラウドを読み解く数字 5、4、3

クラウドの標準として最も多く使われる資料は、アメリカ技術標準協会 NIST(U.S. National Institute of Standards and Technology) の NIST Working Definition of Cloud Computing(NIST 800-145) だ。NIST はクラウドコンピューターを 5 つの必須的な特徴と 4 つの展開モデル、3 つのサービスモデルに区分して説明している。



クラウドコンピューターに対する NIST の定義 (出展: 2011. 11. US NIST)

5: クラウド 5つの特徴

1) リソースの共有 (Resource Pooling)

2) ブロードネットワーク接続 (Broad Network Access)

3) オンディマンド・セルフサービス (On-demand Self service)

4) 弾力性 (Rapid Elasticity)

5) 測定性 (Measured Service)

クラウドの最大の特徴はすべてのコンピューターリソース (Resource) が多数のユーザー (Multi Tenancy) と共有 (Pooling) されるということ。演算を担当する CPU、主記憶装置であるメモリー、ハードディスクのようなストレージなどすべてのリソースはユーザーが必要な分だけ提供される。そして提供されたリソースやサービスは、ネットワークを通じてどこからでもアクセスして使用できる (Broad Network Access)。
もしコンピューターリソースを増設する必要があるのなら、他人の力を借りずに自分で解決できる (On-Demand Self-Service) し、不要になればすぐに使用を中断できるため迅速で柔軟な対応が可能だ (Rapid Elasticity)。共同のリソースを時空間の制約なく利用するために必要なリソースの使用料を払う。これによりクラウドサービスは使用量に対する測定を基本にしている (Measured Service)。

4: クラウド 4つの展開 (Deployment) モデル

1) 公開型クラウド (Public Cloud)

2) 閉鎖型クラウド (Private Cloud)

3) コミュニティクラウド (Community Cloud)

4) ハイブリッドクラウド (Hybrid Cloud)

クラウドのメリットはリソースを複数のユーザーが一共有する点にあるが、その一方でクラウドを忌避させる最大の理由にもなっている。クラウドの管理者やサービスを共有する対象が他社の者ならば、そのシステムを 100% 信じることができるだろうか。クラウドを一緒に使用する者の中にハッカーや犯罪集団がないと言い切れるだろうか。このことから登場したのはクラウドサービスの機能的なメリットはそのままに、他の組織からの接続を制御してセキュリティ問題を排除する展開方式「閉鎖型 (Private) クラウド」である。逆にお金をもらって提供する共用リソースという一般的な概念で運営されるクラウドを「公開型(Public)」クラウドと言う。クラウドシステムは一度構築すれば様々なシチュエーションで活用できて自由度が高く優れた点が多いが、初期の構築段階ではどうしても大掛かりな作業が必要となる。またクラウドをきちんと使いこなすためには、適正水準のシステムの余裕を確保する必要があるがこれを個人で負担するのは厳しい。これにより事業分野が類似したり特定のフレームで区分できる (系列社同士など) 組織同士で運営するクラウド展開方式もある。これを「コミュニティ(Community) クラウド」と呼ぶ。最後に企業の要望によって公開型、閉鎖型、コミュニティ型を適切に混ぜて使い分けるタイプを「ハイブリッド (Hybrid) クラウド」と言う。

3: クラウド 3つのサービス提供 (Delivery) モデル

1) Software as a Service (SaaS)

2) Platform as a Service (PaaS)

3) Infrastructure as a Service (IaaS)

クラウドサービスにも段階があり、最もシンプルなサービスは核心的なインフラのみレンタル (Infrastructure as a Service) すること。サーバーとネットワークアプライアンス、ストレージ、これらを運営する空間などハードウェア的に密接なリソースがこのサービス対象に当たる。ソフトウェア要素はこれらハードウェアインフラを、ユーザー観点から便利に使用できるように連結ポイントを提供する API (Application Programming Interface) 程度に過ぎない。このモデルは建物で例えるなら電力と水道など基本的な設備は整っているが、鉄筋コンクリートそのままに内装工事をしていない状態でレンタルするようなもの。内装を施して家具を入れ、どの用途で使うかは借りた者次第である。IT 観点ではインターネットに接続し何もインストールされていない真っ白なサーバーの状態といえる。サーバーに何をインストールするか、どのようなサービスを運営するかはすべてユーザーの責任であり、インフラ運営以外のすべての問題に対してもユーザーが解決しなければならない。IaaS でよく知られた例にはアマゾンの EC2 (Elastic Compute Cloud) や S3 (Simple Storage Service) がある。

IaaSが最もデフォルトなサービスなら最上位の SaaS (Software as a Service) とは、ユーザーが利用するアプリケーション階層までクラウドで提供するサービスのこと。よく知られたケースとしては Google の Gmail やアマゾンの AWS(Amazon Web Service) がある。このサービスはユーザーが直接開発したりメンテナンスする必要がなく、そのまま使用すればよい。SaaS タイプの場合は管理負担やセキュリティを含む各種問題に対する責任も非常に少ない。IaaS や PaaS に比べてユーザーの介入する部分が少ないため、各種管理負担が少ないことがメリットだ。

IaaS と SaaS の中間タイプ PaaS (Platform as a Service) は、ハードウェアインフラ以外にもユーザーがアプリケーションを開発するために必要なソリューションまで一緒に提供するサービスを意味する。遊びで例えるなら、IaaS は駆けっこ遊びができる校庭だけ提供されることで、SaaS は玩具の飛行機や自動車、人形といった完成品を与えること。PaaS はレゴのように何かを直接作れる材料を提供することになる。PaaS の代表的な例 Google の App Engine の場合、ユーザーには DB API (Application Program Interface) と Python/Java/php などをベースにした開発フレームワークが提供され、自分だけのアプリケーションを作成しては完成したプログラムを Google クラウドで運営することができる。営業ソリューションで有名なセールスフォース・ドットコムも、よく PaaSの事例に挙げられるが php、java、.net ベースの開発ツールはもちろんモバイルサービスを構築するための SDK を含むセールス・ドットコムに連動可能なアプリケーションを、ユーザーが開発できるようにサポートしている。

クラウド導入のための 14 のセキュリティ要素

現在クラウドのセキュリティ分野で最も知られた組織は CSA (Cloud Security Alliance) だ。特定国家に所属していない非営利団体で、会員数は世界約 5万人。クラウドセキュリティに関する基準とガイドを提示することを目的に設立された。CSA で発行されたクラウド・セキュリティガイドは現バージョンで 3.0 までリリースされたが、CSA はこの資料の中でクラウドのセキュリティ検討要素を 14 のドメインに分けて提示している。公開型 (Public) や閉鎖型 (Private) クラウドシステムを構築する場合も、このガイドを参考にすれば大きく役立つはずだ (参照: https://cloudsecurityalliance.org/research/ccm/)。

ドメイン 01	**クラウドコンピューター アキテクチャー・フレームワーク**	前述した「クラウドを読み解く数字 5、4、3」を参照。 クラウドの展開タイプと提供するモデルによってユーザーの責任領域が異なり、セキュリティを適用するプロセスにも差が生じる。クラウドコンピューターの基本構造を説明。
ドメイン 02	**ガバナンス及び 全社危機管理**	クラウドは基本的に提供者とユーザーが所属する組織が異なることを前提にするので、セキュリティに関する相互合意事項や脅威に対する分析と対応プロセスがきちんと合意されるべき。ガバナンスは提供者やユーザーあるいは第三者との関係まで考慮する。
ドメイン 03	**法的懸案: 契約及び電子的証拠収集**	クラウドは適用過程や運営中に問題が発生する場合、データシステムの運営者とユーザー間深刻な法的問題が発生する可能性もある。韓国ではインターネット業社が顧客データを同意なしに海外のクラウドサービス業社へ移管する場合は、違法行為となる。もしデータ損失が発生した場合は、電子的証拠を保管する法規も大きな問題になりかえない。 このため国内外の各種規制を事前に検討し、提供者とユーザー間の法的責任範囲を SLA (service level agreement) に反映すべき。
ドメイン 04	**コンプライアンス及び監査管理**	ドメイン 4 はドメイン 2 (ガバナンス) とドメイン 3 (法的懸案) を繋ぐ役目をする。 法的基準をまとめることがドメイン 3 ならば、それに対する対応システムを整えることがドメイン 2 (ガバナンス) であり、実行される過程こそコンプライアンスだからだ。 提供者に求められるコンプライアンスをモニタリングするためには、適切な監査プロセスが事前に樹立されているべきだ。
ドメイン 05	**情報管理及びデータセキュリティ**	情報セキュリティの重要な目的は、システムとアプリケーションの基礎データを保護することにある。伝統的な IT インフラセキュリティ同様クラウドもまたポリシーとコントロールの手順、関連するセキュリティソリューションについて基準をまとめる事が重要だ。 本ドメインでは IaaS から SaaS に至る各サービスモデルの構成要素とセキュリティ事項を説明している。特にデータ暗号化と通信セキュリティは既存システムでも重要だが、全面的にネットワークに依存するクラウドサービスではさらに注意を払う必要がある。

ドメイン 06	相互運用性及び移植性	クラウドはハードウェアの物理的階層と独立した多様なサービスが運営される。異なる機種の環境で運営された顧客サービスやデータが移管されたり、逆にクラウドサービスの終了により他社に既存のデータを移す場合もある。これはクラウド同士や顧客とクラウドサービスの間でスムーズにデータが運用されて移植が可能であるかどうかが、重大なチェック要素になる。
ドメイン 07	オーソドックスなセキュリティ、事業継続性、インシデント復元	このドメインはオーソドックスな IT インフラのセキュリティと大差ない。クラウドも物理的環境を整えたり災害に対して備える必要があるからだ。注目すべきはクラウドの場合は人的資源を物理的なセキュリティ要素として扱うという点だが、ユーザーが物理的にクラウドシステムに接近する機会がほとんどないため、提供者の人的資源を制御することが重要なポイントになるということを理解すべきだ。
ドメイン 08	データセンター運営	IT インフラを運営するために設計された建物を「データセンター」と言う。ドメイン 5 から 7の領域で扱う要素の中で最もベースになる物理的セキュリティ要素として、建物と施設の運営問題を取り扱う。
ドメイン 09	インシデント対応	インシデント対応は情報セキュリティ管理において最も基本的な要素の一つ。大規模なクラウドサービス企業では、一般企業で直接運営するよりもずっと高い水準でセキュリティ対策を取っているが、それでもインシデントは発生している。アマゾンを含めて Google とマイクロソフトのクラウドもエラーとハッキングのインシデントが発生した (参照:http://www.ciokorea.com/news/9447)。これはクラウドの提供者一方だけの問題ではなく、入居した顧客に発生したインシデントだとしても多数のユーザーが使用するクラウドの特性上、インシデント発生時の対応プロセスは非常に重要だ (フォレンシック過程で他ユーザーのデータ侵害可能性など)。
ドメイン 10	アプリケーションセキュリティ	クラウドはサービス提供モデル別にアプリケーションの運用責任や作動水準が異なるため、CSA では「ソフトウェア開発周期セキュリティ」-SDLC(Secure Development Life Cycle)を強調する。運営プロセスで一旦問題が発生すると影響が大きいため、開発過程のコードレビューとセキュリティスキャンを含むプリテストを徹底的に行うことを要求する。
ドメイン 11	暗号化及びキー管理	ドメイン 11 はドメイン 5 で触れた暗号化について詳細に説明している。適切な暗号化と拡張性のあるキー管理方法、リソースへのアクセス及びデータを保護、身元を確認する際に暗号化及びキー管理が必要な理由などを詳細に紹介している。

ドメイン 12	**身元確認 権限設定 接続制御**	クラウドで忘れてはならないキーワードは、マルチテナント (Multi-Tenancy) とプロビジョニング (Provisioning) だ。マルチテナントは訳せば「多重顧客」で、前述したクラウドサービスを利用する多数の利用者を指している。これといって特別な単語ではないが、クラウドは一つのシステムの中で複数のユーザーが共存しても、自分だけの独立した環境で使用していると感じられるように作成する必要があるため、多重運営環境を提供する高度化された技術そのものを意味することがある。プロビジョニング (Provisioning) は整備されたリソース (コンピューターリソース及びユーザーアカウントなど) を提供すること。ドメイン 12 は、このようなマルチテナント環境で身元確認と権限設定、接続制御などのセキュリティの懸案を扱っている。
ドメイン 13	**仮想化**	クラウドの強みは IT インフラの物理的構成をユーザーが深く知る必要なく、多様なソフトウェアの開発/運営が可能だという点だ。このような構造を可能とする技術的背景には「仮想化」がある。多数のユーザーがそれぞれ異なるアプリケーションと運営ソフトウェアを起動するため、クラウドサービスはハイパーバイザー (hypervisor) という論理的プラットホームを最下位レイヤーに位置づける (ホテルで言うなら建物の礎だと理解すれば良い)。だがもしハッカーが個別のユーザーシステムではなくハイパーバイザーを攻撃して占拠すれと (ホテルの礎を崩すこと) どうなろうか?
ドメイン 14	**サービスとしての セキュリティ (Security as a Service)**	CSA ガイドバージョン 3.0 で新規追加されたドメインは、用語さえ真新しい SecaaS (Security as a Service) だ。概念はシンプルで、ソフトウェアやインフラをサービスとして提供するようにセキュリティもまたクラウドサービスの一つとして提供できるということ。 一例として企業でセキュリティソリューションとして導入するソフトウェアを見てみよう。クラウドのマルチテナント環境に入居した会社ごとに個々の環境に合わせたソフトウェアプログラムを運営するよりは、クラウドのハイパーバイザーレイヤーでセキュリティ機能を運用した方が効率的だ。統合認証 (SSO) や脆弱性点検、アカウント管理などの機能もまたクラウドで提供される。今後多くの企業が IT サービスをクラウドに移行すると予想するなら、運営に必要なセキュリティもまた重要なクラウドサービスの一つとして位置付けられるだろう。

ここまでクラウドの概念と特徴、セキュリティドメインについて見てきた。クラウドは完全に新しい概念というよりは、昔から存在した様々な良い技術が蓄積されて「クラウド」が成立し、活性化されてきたケースだ。今後クラウド技術に対する関心はますます高まり、そのメリットを活かしてさらに拡張していくだろう。アンラボもまたトータルセキュリティ企業として、クラウドを活用してさらに便利なセキュリティサービスを提供できるよう努力していくつもりだ。

http://www.ahnlab.co.jp

http://global.ahnlab.com

http://www.ahnlab.com

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒101-002 東京都千代田区外神田4-14-1 秋葉原ＵＤＸ ８階北 | Tel：03-5209-8610 (代)