「クラウドが当たり前」の今だからこそ整理したい
パブリッククラウドのセキュリティ基礎知識

今や「クラウドサービス」は企業の IT システムを考える上で不可欠な要素です。しかしその一方で、「セキュリティ」に対する漠然とした不安から、クラウド活用に踏み切れていないというケースもあるのではないでしょうか。ここでは、ユーザーが把握しておきたい「パブリッククラウド活用にあたってのセキュリティへの考え方」をまとめます。また、後半では、比較検討を進める際に確認しておきたいポイントを「チェックリスト」として紹介します。

ビジネスに必要な IT リソースを“必要な時に、必要な分だけ”調達でき、運用管理コストを削減できるパブリッククラウドサービスは、今や多くの企業の IT ポートフォリオに欠かせない存在になりました。適用範囲も「短期プロジェクト」「情報系システム」の一部といったところから、より重要な「基幹系システム」にまで広がりを見せつつあります。初期において、企業によるクラウド導入の高い障壁になっていた「セキュリティ」に関する理解が進んだことが、現在の「クラウド活用が当たり前」といった状況への変化を促した要因のひとつでもあります。

そうした状況がある一方、現在でもパブリッククラウドのセキュリティに対する「漠然とした不安」があるせいで、積極的な活用に踏み出せていないという企業も多いようです。たしかに、自社で物理的なハードウェアを「所有して運用」する「オンプレミス」と、ネットワークを通じて「利用」する「クラウド」では、ユーザーが運用にあたって配慮しなければならない「セキュリティ」に対する考え方が変わってきます。そのことが、導入をためらわせる「漠然とした不安」の原因になっているのではないでしょうか。

ここではあらためて、ユーザーが理解しておきたい、パブリッククラウド活用時の「セキュリティ」への基本的な考え方を整理してみたいと思います。これらを正しく理解しておくことは、自社の要件に合った形で、クラウドのメリットを存分に活用していくためのヒントになるはずです。

パブリッククラウドのセキュリティへの「漠然とした不安」をなくす考え方

●なぜクラウドだと不安なのか？

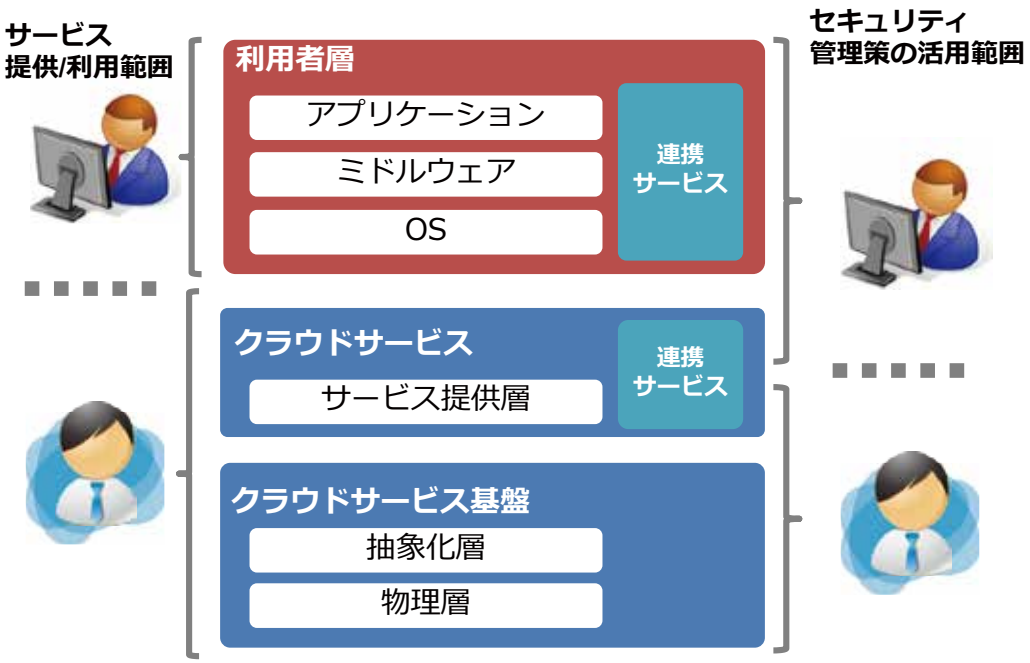
企業が IT システムを導入する際、システム要件の中でセキュリティについても定義をしていることでしょう。今までのオンプレミスの場合、データセンターやサーバなどのインフラストラクチャからシステムのアプリケーションの開発、運用まで企業に裁量がありました。自社で全てを賄うのが困難な場合には SIer に委託をすることもありますが、SIer の選定も含めて、自分でコントロールをすることが可能でした。

一方で、クラウドの場合は異なります。近年クラウドサービスは機能拡充が進み、大手パブリッククラウドサービスでは、「機能的には」オンプレミスと比較して劣ることは殆どなくなってきています。オンプレミスで稼働していたシステムをそっくりクラウドに移行するという事例も少なくありません。しかしクラウドの場合、クラウド利用者はあくまで機能を利用するのみで自分で詳細の仕様を指定することは多くの場合、できません。従ってクラウド利用者は自分でサーバの型番や要求性能を指定することはできませんし、どこのデータセンターでサービスが稼働しているかを把握できないことも少なくありません。さらには、クラウドサービスのサービス運用体制について要求することも、多くのパブリッククラウドの場合は困難です。自らの要件に見合うクラウドサービスを選択するということが重要になってきます。

こういった「できない」「わからない」といった自らの決定権の縮小がパブリッククラウド利用に関する不安の本質といっていいでしょう。では、すでにクラウドを利用している企業はそういった不安をどのように乗り越えているのでしょうか？

●クラウドはセキュリティもお任せできる？

パブリッククラウドを利用する際に、セキュリティに関して利用者が考慮するべきことには２つの観点があります。まず１つは、事業者が何をしているか、もう１つは利用者が何をしなければならないか、ということです。例えば、どんなに利用者が高いセキュリティレベルでシステム運用を行っていたとしても、事業者のサービス運営がしっかりしていないと、情報漏洩のリスクを低減することにはならないでしょう。その逆も同様に、クラウド事業者が堅固なセキュリティを誇るクラウドサービスを提供していたとしても、利用者が全くセキュリティを考慮した利用をしなければ、例えば“サーバー乗っ取り”などの被害に遭いやすくなることもあるでしょう。そういった、利用者と事業者双方でセキュリティを担保するという考え方は「共同責任モデル (Shared Responsibility Model) と呼ばれています。この「共同責任モデル」は、一般的なパブリッククラウドサービスにおける基本的な考え方になります。利用者と事業者の間の責任の切り分けについてはサービスによって異なりますが、パブリッククラウドサービスの場合は、クラウドの提供基盤に関するセキュリティは事業者が、仮想サーバ領域やネットワーク環境、データ領域といった自身の利用する環境についてのセキュリティは利用者が責任を負う、となっていることが多いです。すべての責任を自社で持つ「オンプレミス」や、契約ベースで責任範囲についてあらかじめ決めておく「ホスティングの SI モデル」との特長的な違いのひとつになりますので、理解しておきましょう。



ここがポイント！

最近では、利用ユーザー側が行うべきセキュリティ対策を「機能・サービス」という形で提供するクラウドベンダーも増えています。たとえば、国内大手の「ニフティクラウド」では、専用線・閉域網のネットワーク接続ポートのサービスや、仮想サーバの脆弱性、ウイルスをチェックするサービスなど、他のベンダーとのアライアンスも含めた様々な機能を提供しています。

ここからは、クラウド利用の際によく挙がる不安はどうすれば解消されるか、「共同責任モデル」の考え方に沿って簡単にみていきましょう。

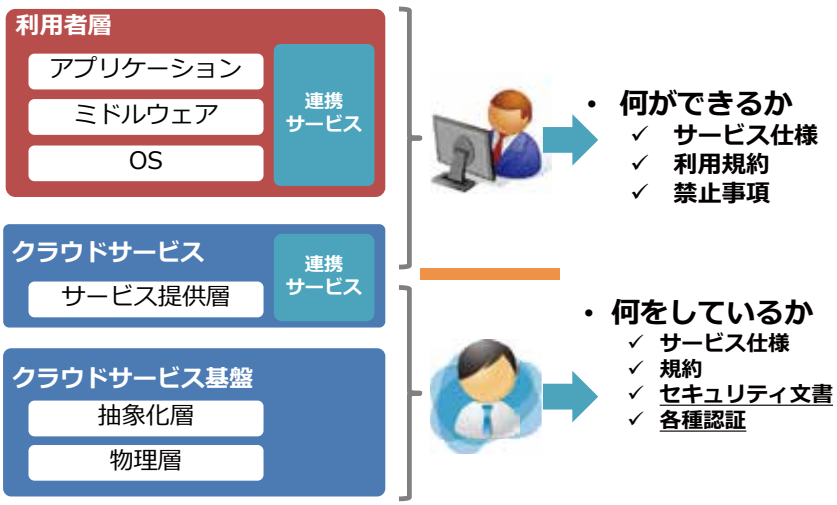
●不安その 1
「外部の第三者に情報が漏れる心配はない？」

このリスクについては、いくつかの観点で見ていく必要があります。

まず、クラウド事業者による情報漏えいのリスクです。多くのクラウド事業者は、厳格な運用管理プロセスを実施しています。クラウド事業者がクラウド利用者の環境に触れることは、実態としてはほとんどないでしょう。しかし、クラウド事業者のサービス運用が本当に安心できるものか、ということは確認が必要です。公開されている情報を参照したり、直接問い合わせたりすることにより、セキュリティ要件に対応しているかを確認することが重要です。外部の第三者からのチェックによる客観的な評価として、制度資格や認定・認証の取得を確認することも有効です。代表的な標準規格、認定制度としては、「ISMS」（情報セキュリティマネジメントシステム適合性評価制度）や「CS マーク」（JASA- クラウドセキュリティ推進協議会による認定制度）などがあります。

次に、クラウドサービスにおけるユーザー環境の保護の仕組みに関するリスクです。パブリッククラウドの場合、多くはマルチテナントで提供されているため、他のユーザーから自分の環境が攻撃や調査などの干渉を受けてしまう可能性があります。そのようなリスクに対して、どのように事業者が対応しているか確認する必要があります。例えば、プライベートネットワークが VLAN などで隔離できる仕組みがあるか、また他のユーザーへの干渉行為が規約によって禁止・制限されているかなどです。サービスの仕様書や利用規約などの記載を注意して確認しましょう。

最後に、クラウド利用者の運用におけるリスクです。例えばファイアウォールの設定に不備があり、不要なポートまで開いていることで攻撃を受けやすい状態になっているといった場合です。多くのクラウドサービスでは、ファイアウォールなど利用者のセキュリティ対策のための機能をサービスの中で提供しています。その他にもウイルス対策ソフトなど、著名なサードパーティ製品をクラウドサービス上で扱えるなど、利用者のクラウド運用負荷を下げるための取り組みがされていることもあります。その上で、クラウドサービスをどのように運用していくかを定め、きちんと管理していくことが重要です。そこには情報漏洩が発生した際に、いかに速やかに検知して対応できるかということも含まれます。情報漏洩に気付けずに影響が広がっていくと、事態の収拾により多くの労力を費やす必要があります。そのような場合も含め、トラブル時の事業者との対応体制についても確認しましょう。



ここがポイント！

クラウドの「情報漏えい」リスクに不安があれば、事業者が取得している制度資格や、認定・認証の取得を確認しましょう。例えば、ニフティクラウドでは以下のページ（http://cloud.nifty.com/policy/security.htm）で、認証取得を外部に公開しています。併せて「VLAN」や「ファイアウォール」といった、クラウド事業者が提供するセキュリティ機能を適切に活用し、トラブル時の対応含めたセキュリティ運用を実施することが重要です。

●不安その２
「クラウドに置いたデータは消失リスクが高い？」

クラウド利用時のデータ消失リスクについても事業者と利用者双方の視点で考える必要があります。

まず、クラウド事業者起因のリスクについては、主に「サービス運用」と「システム障害」の観点があるでしょう。

「サービス運用」については、クラウド事業者が運用時の操作（オペレーション）ミスなどで誤って消してしまうリスクが考えられます。これは前項同様に「認定制度」などで事業者の運営体制について確認するのがよいでしょう。次に「システム障害」は、クラウド基盤を構成するストレージ装置などが物理的に壊れてしまい、データが取り出せなくなるといったことが考えられます。これは、クラウドサービスのアーキテクチャに関わる問題です。

最近ではほとんどのクラウドサービスが、物理機器を冗長化した上でデータ保護の仕組みを導入しているため、物理障害によるデータ消失の例はほとんど聞かれません。しかし、クラウドサービスの障害時に利用者がどれだけ迅速にサービスを復旧できるかはサービスによって異なるところです。例えば、サーバーイメージをバックアップする機能や、バックアップ環境として安価なストレージを活用することは速やかなサービス再開には有用でしょう。

また、クラウド利用者起因のリスクについては「システム運用」と「ベンダーロックイン」の観点があるでしょう。「システム運用」については前項で触れた通り、利用者自らがきちんと運営体制を整備する必要がある。その際に、クラウドサービスでバックアップの機能など運用をサポートする機能が提供されているとフェイルセーフとして有効です。

最後に「ベンダーロックイン」については、事業者によるサービス終了が挙げられます。当然のことながらクラウドサービスは慈善事業ではなく、不採算なサービスはいずれ終了してしまいます。有名な例では 2013 年に老舗クラウドストレージサービスの nirvanix 社が突然の経営破たんおよびサービス終了を発表しています。また、最近では事業者によって、利用規約に抵触した利用者のアカウントを突然停止されるクラウドサービスもあるといいます。そのような事態により自分のデータを急に取り出せなくなることは非常に問題です。事業者選定の際には事業継続性だけでなく、サービス終了時の告知など取りうる対応を確認しておくことが重要です。

ここがポイント！

クラウドサービスでのデータ消失は「絶対にない」とは言えませんが、そのリスクは、自社でデータを管理する場合と比較して、高くもありません。クラウドにデータを保存する場合も、従来行っていたような「バックアップ」の計画をユーザー側で用意しておくことで、データ消失のリスクは大幅に削減できます。その場合、クラウドサービス側が用意している障害対策との複合効果で、自社で管理している場合よりもデータの可用性が高まるケースも多いはずです。

クラウド利用の前に確かめたい「クラウドセキュリティ」チェックリスト

今回紹介したクラウド利用の際のリスクとその対策は、あくまで一部にすぎません。また、クラウドサービスの利用に限らずセキュリティ対策は、あくまで対象のシステムに潜むリスクに応じて適切に施すものであり、ここで挙げたものを全て実行すれば必要十分という訳ではありません。クラウドサービスに関するセキュリティ上のリスクについては経済産業省の「クラウドセキュリティガイドライン　活用ブック」にまとまっています。その中にはクラウド利用者がどのようにクラウド事業者を選択し、システムを構築するのが望ましいかということについても触れられています。

以下では、その中でも特に見過ごされやすい６つのポイントを紹介します。

その１
「管理画面」に複数のセキュリティ対策があるか？

一般的に、クラウドサービスの管理画面にアクセスする際には「ID ／パスワード」による認証が行われます。しかし、企業で利用する場合、「ID ／パスワード」認証だけでは不十分と言えます。現在では、IP アドレスによる管理画面へのアクセス制限や、経路認証などを複数組み合わせて提供するクラウドサービスが増えています。逆に、「ID ／パスワード」による認証のみしか利用できないサービスは避けるべきでしょう。

その２
「ログ」は取得できるか？

監査への対応の際に、システムの「操作ログ」が必要になる場合があります。その際にクラウドの機能、例えばファイアウォールなどへのアクセスログを取得できるかどうかは、クラウドサービスによって異なります。必要なログを入手できるかどうかについて、導入前にチェックしておきましょう。

その３
障害時の対応フローに問題はないか？

サービスに障害が発生した場合の第一報がどのような形で届くのか、その後のフローはどうなっているのかなどは、事前に確認しておくことをお勧めします。ビジネスで利用するシステムが「止まった」ときの対応品質は、システムが動いている場合のサービス品質と同等以上に重要です。ニフティクラウドでは、発生した「障害のレベル」に応じて、ユーザー自身が通知の要不要を選択できる機能を無償で提供しています。

その４
「データセンター」のセキュリティ対策状況は？

「停電時の運転継続時間は？」「データセンター入場時の認証方法は？」など、データセンターの運用に関する基準が、自社のセキュリティ要件に合致するかどうかは、事前に確認しておくとよいでしょう。ニフティクラウドでは、データセンターごとのセキュリティ対策や災害対策をホワイトペーパー（http://cloud.nifty.com/pdf/security_whitepaper.pdf）として公開しています。

その５
外部からのサイバー攻撃への対策はできるか？

外部からの攻撃に対する対策機能は、オプションの有償サービスとして提供しているベンダーがほとんどです。ニフティクラウドの場合、外部のパートナーとのアライアンスに基づいて、「IPS/IDS」「ウイルスチェック」「WAF」といったセキュリティサービスを提供しています。

（参考リンク）
・IPS/IDS、ウイルスチェックなど
http://cloud.nifty.com/service/dsaas.htm
・WAF
http://cloud.nifty.com/service/waf.htm

その６
クラウド上のリソースに対するアクセスコントロールは可能か？

「特定のアカウントがアクセスできるリソースを、サーバ操作のみに限定する」などといった形で、アカウントごとの権限をロールで管理する仕組みを提供しているクラウドサービスも出てきています。現時点で、対応しているクラウドサービスは多くありませんが、ニフティクラウドでは「マルチアカウント」という機能で同様のことが可能になっています。

パブリッククラウドサービスの選択・利用は、機能や価格だけでなくセキュリティも考慮することが重要です。今回ご紹介した「漠然とした不安」の解決方法や、「クラウドセキュリティ」のチェックリストをぜひお役立てください。