解 説 4

クラウド・コンピューティングにおけるセキュリティー対策

クラウド・コンピューティングのセキュリティー・レベルは格別低いということはありません。システムのセキュリティーを守るべき手段が正しくそろっているからです。特定の用途に限定したアプリケーション・サービスを行っているSaaS（Software as a Service）やアプリケーションのプラットフォームを提供するPaaS（Platform as a Service）の中には、極めて強固なセキュリティー対策が提供されているものがあり、安心して利用することができます。こうしたサービスではセキュリティー管理もサービスの一部として統合されているからです。

しかし、IBM SmarterCloud Enterprise（以下、SCE）やAmazon EC2のようなIaaS（Infrastructure as a Service）クラウドのサービスではすべてを自分で管理しなくてはならないという自治性の側面があります。これまでの企業内データセンターでは、インターネットとの接続によって生じるセキュリティーの管理は、セキュリティーの専門家によってなされてきました。インターネットに直結したIaaSクラウドの利用者は、これまでのサーバー管理の領域を超えて、ネットワーク・セキュリティー、サイバー攻撃への対抗手段の必要性を理解し、対策を講じて、社会的な責任を果たさなくてはなりません。

本稿ではIaaSクラウドのセキュリティー対策について解説します。

❶ 自由と引き換えの責任

クラウド・コンピューティングへの不安として幾度となくセキュリティーの課題が取り上げられていますが、現実はどうでしょうか。

サーバー管理者：
「Windows ServerのAdministratorのパスワードを“なし”にしたんだけど」
SE：
「…」
サーバー管理者：
「だって、パスワード面倒なんだよね。
これまではそうしていたよ」
SE：
「…で、何をお守りすればよろしいのでしょうか？」

この例は極端なものだとしても、これまでデータセンター内で保護されてきたサーバー管理者のセキュリティー意識とはこうしたものかもしれません。IssSクラウド導入時、サーバー・インスタンスを作成しアプリケーションやミドルウェアを導入する際にインストール権限としてrootやAdministratorなど特権ユーザーのパスワードをセキュリティーの知識のない作業者に手渡してしまったり、インストール・スクリプトが正常に動かないために危険なアクセス・ルートをオープンにしてしまったりといったセキュリティー事故が報告されています。これらは、IaaSクラウドのセキュリティーに対する意識の問題であって、IaaSクラウドの技術的な危険性を示しているものではありません。繰り返しますが、クラウド・コンピューティングは格別危険な環境ではありません。しかし、IaaSクラウドのセキュリティーを守るためには、サーバー管理者はこれまでのセキュリティーへの意識を変える必要があります。

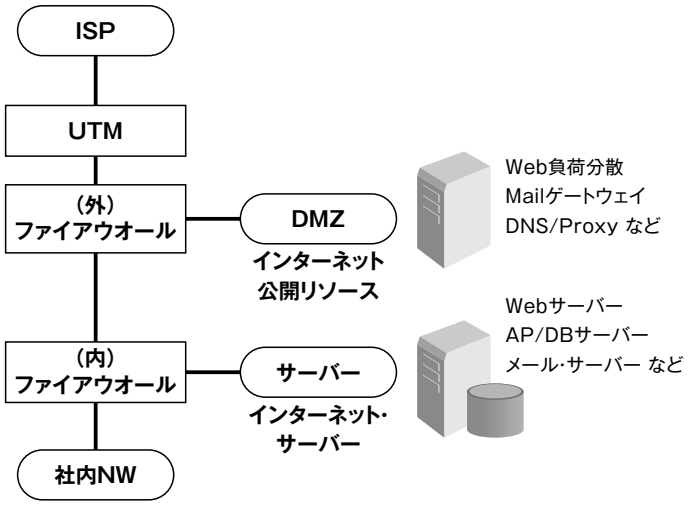
パブリックなIaaSクラウドではセキュリティーにかかわる判断は利用者自身=インスタンスのオーナーに任されています。これまでのインターネットに接続されたシステムの管理者は教育を受けた専門家に限られてきましたが、クラウド・コンピューティングの環境では多くの社内ユーザーがインターネットに接続されるようになりました。クラウド・コンピューティングのポータル・サイトにアクセスして新規にサーバーを作り出すことのできる社員は数多く存在します。このセルフサービスによる柔軟性がクラウド・コンピューティングの命だからです。そのため、クラウド・コンピューティングの利用者全員がインターネット上の脅威と戦わなくてはならないのです。しかし現実には一般市民が戦場にのこのこ入ってきているような無防備さも目立ってきています。クラウド・コンピューティングの一段の普及のためにも、インターネットのセキュリティー意識の一般化を進

めることが必要です。

❷ インターネットに直接接続しているということ

NIST（National Institute of Standards and Technology：米国国立標準技術研究所）の定義によると、「クラウド・コンピューティングの最も重要なアクセス要件はインターネットに接続していることである」とされています。著者はこれまでネットワーク・エンジニアとして、お客様のインターネット・サイトやインターネット・サービス・プロバイダーのセキュリティーを守るインターネット接続のアーキテクチャーやテクノロジーを数多く実装してきました。クラウド・コンピューティングの利用者は、ネットワークやセキュリティーのエンジニアがどれだけの慎重さでインターネット上の脅威からネットワークを保護してきたのかということを知る必要があります。なぜならインターネットに直接接続されたIaaSクラウドの環境では、構築したサーバーは直接インターネットに接続された状態で提供されるからです。

ネットワーク・エンジニアによって設計され慎重にテストされたファイアウオールでさえ、たった1つの設定ミスがセキュリティーを台無しにしてしまいかねません。ネットワーク・エンジニアはHTTP（HyperText Transfer Protocol）とSSL（Secure Socket Layer）以外のポートをインターネットに対してオープンにする要求には極めて慎重に対応します。ログインやFTP（File Transfer Protocol）などのプロトコルには複雑な設定が必要だということを知っています。グローバル・アドレスを直接サーバーに付与する危険を知っています。決して社内の重要なサーバーに直接インターネットからの通信を送ることはせず、DMZの中継サービスを経由させます。さらに、ネットワークのファイアウオールは万能でないことを知っています。アドレス・フィルターやステート管理などの基本機能だけでは守れない新たな脅威が日々増えているからです。



ISP : Internet Service Provider
UTM : Universal Threat Management
DMZ : インターネット緩衝地帯
DNS : Domain Name Server
AP/DB : Application/Database

図1. インターネット接続のネットワーク構造の例

表1. インターネット接続の注意点（例）

● HTTP/SSL以外のポートは開かない。 ●例外のポートは十分な審査の上で対処する。 ●平文パスワードは流出させない。 ●グローバル・アドレスはすべて（外）ファイアウオールでNAT対応をする。 ● DMZにはコンテンツを置かず、リレー機能に徹する。 ● DMZサーバーは厳重にハードニングする。

図1に示したのが一般的なインターネット接続のネットワークの構造です。ファイアウオールはサーバーへのアクセスのフィルタリングを行います。また、正常でないTCP/IPの振る舞いを遮断するステートフル・インスペクション機能や後に述べるようなアドレス変換機能を提供します。UTM（Unified Threat Management）は通常のファイアウオールでは検知できない不正なアクセスのパターンをスキャンするIDS/IPS（侵入検知／防御機能）などで高度な攻撃に備えています。こうした専門機材を利用しながら、危険との距離に応じてネットワークをゾーニング（領域分け）することにより社内ネットワークは守られています。**表1**の基本ポリシーは極めて一般的なネットワーク防御に必要とされる方針です。（外）ファイアウオールではインターネットと接続するためのアドレスをすべて管理します。ファイアウオールのセキュリティー・ポリシーが許可した通信のみがNetwork Address Translation（以下、NAT）機能によりグローバル・アドレスからプライベート・アドレスに変換されて社内の資源にアクセスするように制限を設けています（**図2**）。こういったNATなどの対策は、本来ISPから借り受けたグローバル・アドレスが変更されてもサーバーに影響しない構造を取ることを目的としていましたが、現代ではセキュリティー管理の側面からも必須の対策となりました。

このように、社内ネットワークはファイアウオールや侵入検知／防御装置とゾーニング、転送技術、暗号化通信技術を中心としたネットワークとセキュリティーのベスト・プラクティスによって堅く守られてきました。この堅牢さの裏側で社内システムの運用を行っている社員のセキュリティー意識がおろそかにされてしまっているかもしれません。データセンターの中ではパスワードの管理ですら、厳密に行われていない例もあります。こうした環境では全 ID で共通のパスワードを設定したり、共用のユーザー ID が利用されていることがあります。また、FTP や TELNET、RSH（Remote Shell）などのパスワードが平文で送られてしまう通信に、平然と root パスワードを流してしまうこともあります。SFTP（SSH File Transfer Protocol）や SSH（Secure Shell）など、データを暗号化して通信することができる方法があるにもかかわらず、「速度が遅い」「手間が掛かる」といった理由でこうした機能を利用しないでインターネット上で操作を行うことは非常に危険です。こうしたことはすべて保護手段の取られたネットワークに守られていた社内データセンターでのみ通用することだったのです。

❸ IaaS クラウドのセキュリティー管理

3.1 セキュリティー・ポリシー

IaaS クラウドに限ったことではありませんが、インターネット上の脅威に対して合理的な防御手段の指針となるのが企業のセキュリティー・ポリシーです。本稿ではセキュリティー・ポリシーの内容について詳細には記しませんが、インターネット上の脅威とインターネットの利用状況を分析し、合理的な防御方針を立案する必要があることはどの企業でも共通しています。

IaaS クラウドの特長は、インターネットに接続されたシステムを誰もが簡単に構築できることです。そのため、企業のセキュリティー・ポリシーは、専門教育を受けていない社員がクラウドを利用する場合でも、インターネット上の脅威について完全に理解できる内容であることが望ましいでしょう。こうした活動ではセキュリティーの専門家からの助言を得ながら社員教育を行うことが重要です。IaaS クラウドの操作を行うためには、標準的なセキュリティーの基礎教育とインターネットとの接続にかかわる基本的な遵守事項、社内のセキュリティー・ポリシーなどを包括的、系統的に教育し、遵守させるためのプロセスとルール作りが必要です。また、IT 環境に変化が生じた場合、セキュリティー・ポリシーが新しい IT 環境に対応したものとなるように、継続的な見直しと更新を実施することが必要となります。

3.2 暗号化技術の活用

インターネットに直接接続しているシステムにおけるログイン／パスワードは、防御手段としてはもはや単純過ぎるでしょう。ユーザー ID やパスワードは高度に洗練された辞書攻撃の危険にさらされています。また、個人のパソコンとは違い、サーバー・システムは常に同じ IP アドレスを用いてインターネットに接続しているため継続的な攻撃を受けやすいと理解しましょう。インターネット上では IP アドレスがアクティブになったら、極めて短時間に（数分から十数分の間に）何らかの攻撃を受けるものと考え

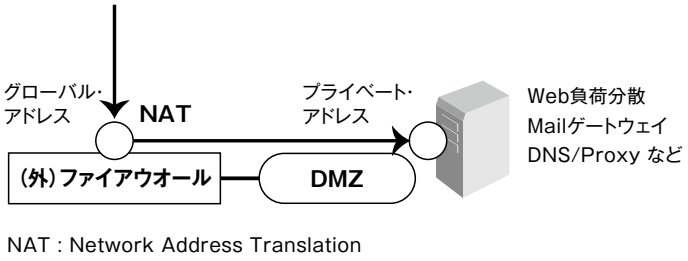


図2. インターネット・サーバーを隠ぺいする

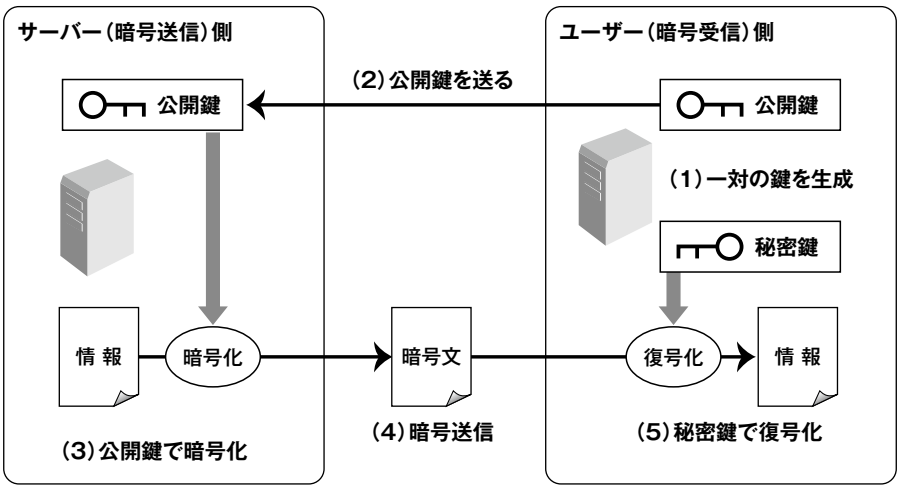


図3. 一方向性を用いた暗号通信の仕組み

なくてはなりません。そのため、サーバーでは暗号化技術を中心とした堅牢なユーザー認証の仕組みが必要です。暗号化技術を用いることで、適切な暗号通信によりシステムが盗聴から保護されるだけではなく、暗号技術が持っている耐改ざん性能がユーザーを確実に特定するユーザー認証機能を提供してくれます。

現代の暗号化技術は秘密鍵と公開鍵によって構成される堅牢な仕組みです。この堅牢さは数学でいうところの一方向性に依存しています。「素数と素数の掛け算の答えから元の素数を割り出すことはできない（極めて困難だ）」という性質を利用したものです。実際の暗号化処理では数百けたに及ぶ大きな素数を利用することで、暗号強度を高めています（**図 3**）。SSH Keyed Login ではサーバー側が公開鍵を用いることで、ログイン時の通信の機密性を守ることができるようになっています。サーバーが公開鍵で暗号化したものを解読できるのは、秘密鍵を持つユーザーだけであり、この方式ならパスワードをネットワーク上に送ることなく確実にユーザーの認証ができます。

インターネットに直接接続している SCE では、公開鍵暗号システムを用いた SSH Keyed Login が標準化されています※1。また、標準でファイアウオールが有効化されており、システムを守っています。こうした防御システムを完全に生かしてクラウド・システムを安全に利用するために、セキュリティー保護のツールが提供されています。

※1　SSH が標準なのは Linux であり、Windows では RDP（Remote Desktop Protocol）の暗号化通信が用いられます。

3.3 プライベート VLAN によるゾーニング

IaaS クラウドでは極めて容易にグローバル・アドレスを持ったサーバーを構築することができます。しかし、前述したようなネットワークの構造的な保護手段は採られていません。各サーバーはそれぞれの責任でサーバーへのアクセスを管理しなくてはなりません。SCE では標準で提供しているセキュリティー保護手段がありますが、これを安易に無効化しないよう、厳重な管理が必要になります。しかし、ミドルウェアの導入やプログラム開発上の必要性から、保護手段を緩めなくてはならない場合もあります。

こうした場合には、ネットワークやセキュリティーの専門家の助言に従い、社内のデータセンター同様にネットワークの構造的な保護手段を講じる必要があります。第一章で述べたようなセキュリティーのゾーニングを行い、**表 1** にあるような実践的な防御ポリシーを実装します。SCE ではこのようなネットワーク構造の構築を支援する、VPN（暗号通信機能）、プライベート VLAN とファイアウオール・イメージ機能を提供し、安全な仮想ネットワーク構造を構築できるようになっています。こうしたファイアウオール機能を用いて、企業内データセンターと同等の安全性を備えたネットワーク構造の中で、安心して IaaS クラウドを利用できる環境作りが重要です。

ファイアウオールの標準的な IP アドレス・フィルターの機能を用いる場合、開発者の IP アドレスが変わるなどの環境変化に対応する必要があります。**図 4** に示すのは SSH のポート・フォワード機能を用いて、SSH の鍵認証の下で安全な通信を行う構成例です。このとき、ファイアウオールにサーバーからのインターネット・アクセスを許可する IP マスカレード機能を実装しておくと、サーバー

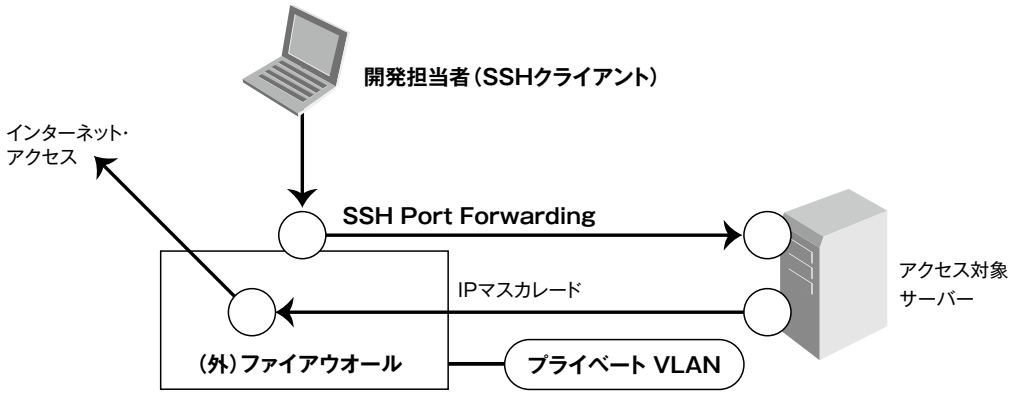


図4. SSHを用いて柔軟な構成を作成する

がインターネット上の修正プログラムやウイルス・パターン・ファイルなどにアクセスできるようになります。

サーバー上のプログラム選択では、Apache や DNS などの数多くのサーバー・プログラムが歴史を重ねる中でインターネット・セキュリティーに対する脆弱(ぜいじゃく)性を発見し、それを継続的に修正して、セキュリティー・リスクを低減させているということに留意します。インターネット上で使うプログラムでも、このような継続的なセキュリティー面での改善と修繕の提供が行われることが必要不可欠です。このような工夫を行うことで、柔軟かつ安全な IaaS クラウドの利用が可能になります。

❹ 最後に

読者の方に誤解しないでいただきたいのは次の 1 点です。本稿ではクラウド・コンピューティングのセキュリティーの危険性をことさらにあおろうとしているわけではないということです。システムの危険性はクラウドであるかどうかにかかわらずインターネットに接続している以上避けて通れない問題です。しかし、正しい対抗策が取られているサイトであれば安全に運営することができます。簡単な例を挙げてみます。SSH ログインへのアタックを例にすると、インターネット上で ping（応答監視コマンド）に応答するように設定されたサーバーへの SSH ログイン・アタックは 1 分間に千回を超えます。しかし、ping への応答を止めた瞬間にアタックは半分に、そしてサーバーをファイアウオールの内側に配備すればアタックはほぼ消滅します。

サイバー犯罪は近年になって巧妙化・高度化しています。日本を代表する、あるいは業界を代表するような有名企業や公共団体などがサイバー攻撃を受けるということは直接的な被害ばかりではなく、サイバー犯罪者の実力を示すことになってしまいます。さらに、踏み台としてほかの企業・団体への侵入に利用されれば、加害者の一端を担ぐことにもなりかねません。インターネット上の脅威への防御対策を行うことは、企業にかかる社会的な責任ということができるでしょう。そして、企業のセキュリティー意識が高まり、インターネットを活用するクラウド・コンピューティング環境のすべての利用者全体にまで十分行き届くことがとても重要です。

クラウド・コンピューティングの目的である、コスト削減、製品・サービスの継続的な開発、ビジネス・モデルの開拓などに対して、統制されたシステムの構築を確実に行っていく必要があります。そのためには、ビジネス・プロセスを再設計することや、これまでのシステムや制度とシームレスに統合していくことだけでなく、本稿でも述べた通り、社会的責任とセキュリティーを統合する必要があります。こうすることで企業のシステムは安全にインターネット上のクラウド環境に広く分散し、インターネットによる IT システムのイノベーションが実現すると信じています。

［参考文献］

［1］ Johannes A. Buchmann（原著），林芳樹（翻訳）：暗号理論入門―暗号アルゴリズム、署名と認証、その数学的基礎，シュプリンガージャパン，ISBN-10: 4431713115（2007-6）.

［2］ 公開鍵暗号で SSH のセキュリティを高める，http://www.jitaku-server.net/ssh_crypto.html

［3］ Turbolinux 11 Server:ユーザーガイド第21章SSH（Secure SHell）サーバー,http://www.turbolinux.com/products/server/11s/user_guide/x9016.html

［4］ 紫関昭光：IBM Smart Business Cloud Enterprise 活用ガイド，廣済堂　Bookgate，pp.79 ページ.

日本アイ・ビー・エム株式会社
クラウド&スマーター・シティ事業 CTO
ディスティングイッシュト・エンジニア 技術理事

山下 克司 **Katsushi Yamashita**

［プロフィール］
1987 年、日本 IBM 入社。適用業務パッケージの開発などを経てネットワーク分野のテクニカル・リーダーを務める。2007 年にネットワーク仮想化技術などの貢献を評価されディスティングイッシュト・エンジニアに認定され技術理事に就任。2010 年からはクラウド・コンピューティング事業の技術統括をするチーフ・テクノロジー・オフィサーに就任し、クラウド・コンピューティングの技術面でのリーダーを務める。