セッション 3
『クラウドコンピューティングに必要とされる情報セキュリティとは』

富士通株式会社
セキュリティソリューション本部 情報セキュリティセンター長

塩崎哲夫 氏

■クラウドコンピューティングとは

皆様こんにちは。塩崎と申します。本日は、現在のクラウドコンピューティングに対する期待と課題、そして、政府も含めた委員会の発足など、その動向についてお話します。

今年（2009 年）の 4 月に米国国立標準技術研究所（NIST）から、クラウドコンピューティングの定義案が出されました。それは、「共用され、設定・調整可能なコンピューティング資源に、簡易かつオンデマンド・ベースでネットワークからアクセス可能な形態のこと。当該コンピューティング資源は、最小限の管理能力やプロバイダーの関与だけで、迅速に提供され、そして解放される」というもので、さらにこの定義案には、クラウドの 5 つの特徴が挙げられています（図表 1）。

1 つ目は、利用要求に応じてオンデマンドで使えること。
2 つ目は、さまざまなプラットフォームからネットワークを通じて使えること。
3 つ目は、「リソースプール」から資源を動的に割り当てられ、マルチテナントモデルにより複数の利用者に提供されること。ASP のように 1 ユーザー1 サーバで提携するのではなく、1 つのプラットフォームを複数のサービス、複数のユーザーで共有すること。そして、その物理的・仮想的資源は需要に応じて動的に割り当てられることです。
4 つ目は、仮想空間やストレージ容量を増やしたり減らしたりする、「スケールイン・スケールアウト」が迅速に、弾力的にできること。
5 つ目は、「計測されたサービス」。資源利用の管理・最適化が自動的に行われることです。資源の利用は、サービス提供者と利用者の両方において、監視、制御され、透明性を持って報告されます。

以前、Amazon EC2 のサービスが停止したときには大きな問題となりました。そこで、Amazon は 10 日ほどでモニタリング画面を立ち上げ、稼働状況を見せるようにしました。今までのクラウドでは、クラウドの中でデータが処理され、利用する側はその仕組みがよくわかりませんでしたが、最近では、クラウドはできるだけ稼働状況やリソース管理、セキュリティ管理について見せる方向に変わってきているようです。

（図表 1）クラウドコンピューティングとその特徴

クラウドコンピューティング出現の背景には、3 つのことが考えられます。
1 番目は、増大する ICT インフラの維持管理費用の増大。皆様もコンピュータ設備をお持ちだと思いますが、その維持管理コストが非常に高くつくと感じられている方も多いのではないかと思います。
2 番目は、ハードディスク・CPU 速度、ネットワークの帯域や速度などの急速な技術進歩です。
3 番目は、最近よく耳にする社会的責任です。特に、グリーン化対応です。実際、データセンターの電力消費量の 45%は、コンピュータの冷却に関連した冷却設備のために使われています。コンピュータ自身の電力消費量は 30%です。センターをばらばらに作っていたのでは、エコの問題は解決できないということです。逆に言えば、サーバやセンターを集約・統合して、オンデマンドで利用すれば、エコに貢献できるということです。また、厳しい経済環境を乗り切る、新たな ICT 投資（IT 管理会計）のあり方もその要素に挙げられています。

クラウドのサービスモデルとしては、SaaS（Software as a Service）や PaaS（Platform as a Service）が挙げられます。SaaS は、利用者が、クラウド事業者のインフラ上のアプリケーションを使用できること。PaaS は、利用者が、クラウド事業者の提供するプログラミング言語とツールを用いて開発、購入したアプリケーションを、クラウドインフラに導入すること。もっとインフラレイヤに近いサービスモデルとしてクラウド事業者から提供されたハードウェア、OS の環境を利用して、利用者が任意のソフトウェアを実行できる IaaS（Infrastructure as a Service）というものがあります。昨年（2008 年）までは、ネットワークを介してマルチテナントで、効率よくパッケージを提供する SaaS がブームでしたが、今年になってからは、さらに下位レイヤーまで自由に使える PaaS や IaaS が注目されています。このときに注意しなければならないことは、バージョンアップはサービスベンダーが責任を負い、インストールしたミドルウェアのセキュリティパッチは利用者が責任を負うなどといった、責任の所在の明確化です。

クラウドの利用者という観点から見ると、クラウドの種類は大きく 4 つあります。
まず、一般にホームページが公開され、誰もが自由に使える「パブリッククラウド」があります。Google などが代表例です。
2 番目に、1 つの組織のために運用される「プライベートクラウド」。プライベートクラウドを自社のデ

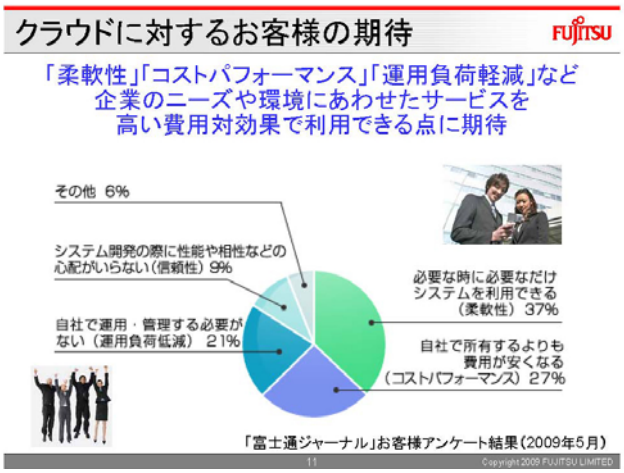
ータセンターで作る場合もあるかと思います。また最近、Amazon では、パブリックの中に 1 つのネットワークセグメントを仕切って VPN（仮想専用ネットワーク）で接続し、隔離された空間を作り、それをプライベートクラウドのようなかたちで提供しています。また Google では企業向けのサービスで、データを置くサーバを Google 側ではなく、ユーザー企業側に置く、セミプライベートクラウドのような形態も提供を始めました。パブリッククラウドでは、自分の情報資産がどこに置かれ、誰が管理するのか、どのようなアクセスコントロールをするのかと言う心配があるので、プライベートクラウドでなければ安心できないといった要求もあるように思われます。
3 番目が、「コミュニティクラウド」です。これは複数の特定の組織で共有されるものです。例えば、米国の医療には HIPPA（Health Insurance Portability and Accountability Act、医療保険の携行と責任に関する法律）というルールがありますが、HIPPA ルールで運用するような共同センターなどが、コミュニティクラウドに近いかたちと言えます。
4 番目に、パブリック、プライベート、コミュニティの 3 つのうち、2 つ以上のクラウドを連携したクラウドとして利用する「ハイブリッドクラウド」があります。これは、セールスフォースのように、XML のインターフェースが提供され、VPN の暗号通信で自分の会社の中に接続できるといったかたちです。

このような中で、セキュリティポリシーは、決して一律ではありません。パブリッククラウドで定義できるセキュリティポリシーは、不正アクセスの監視や ID・パスワードによる認証・アクセスコントロールですが、より業務に依存した、より細かな認証やアクセスコントロールが必要となると、次第に企業・組織が所有するプライベートクラウドの形態になっていくのではないかと思います。

クラウドの利用が想定される業務としては、ウェブやアプリケーションサーバとしての業務、メールなどのコラボレーションツール、CRM（顧客情報管理システム）、SFA（営業情報管理システム）などの業務アプリケーションが挙げられます。また、バックアップなどの共用ディスクとしての利用も、大きく期待されています。さらに、一時的なバッチ処理。例えば、ニューヨークタイムズが自社の新聞記事を PDF の電子メディアに変換するとき、Amazon EC2 サービスを利用した例は非常に有名ですが、そうした一時的ななバッチ業務に大変向いていると思います。また、最近多くなっているのが、開発環境や災害対策のためにバックアップセンターとして利用したいというご要求です。ただ、クラウドの料金は、長期的な利用ではまだ安いとは言えません。3 年以上使用する予定であれば、自社で持つほうが安いケースも少なくないため、その選択には十分な検討が必要と思います。

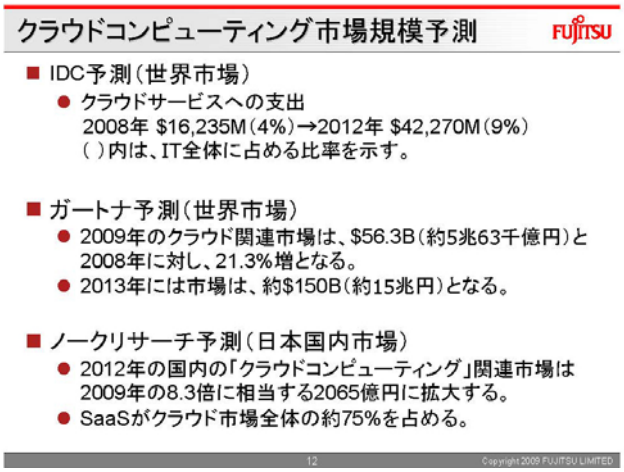
■クラウドへの期待

クラウドへの期待としては、大きく 4 つのことが考えられます。まず、1 つが、IT 投資リスクの低減。2 つ目は、メモリやサーバ、ネットワーク帯域を増やしたい、ストレージを増設したいといったご要求への柔軟性な対応です。3 つ目は、インストールやセットアップといった、さまざまな IT リソースの管理を短縮するスピードアップ。そして、4 つ目が、運用からの解放です。『富士通ジャーナル』（2009 年 5 月号）でのお客様アンケートのトップも、柔軟性、コストパフォーマンス、運用負荷の軽減に対する期待となっています（図表 2）。



（図表 2）クラウドに対するお客様の期待

日本国内での市場予測には、IDC やガートナーほかさまざまな予測があります。金額的に大きな予想を出しているリサーチ会社もあるようですが、富士通のクラウドサービスは 2015 年には 20%以上のマーケットシェアを占めたいと考えています。
また、IT 投資に占める比率が、徐々にクラウドに移行していき、関連市場も 21.3%以上増加する、2013 年には 15 兆円になるなどといったことも予測されています（図表 3)。



（図表 3）クラウドコンピューティング市場規模予測

このような環境の中で、さまざまな研究会やコンソーシアムなどが活動を始めています。従来クラウドと関係が薄かった組織でも調査・研究が進み、サービス内容や技術といったレベルでの標準化が進んでいます。例えば、IBM を中心に今年初頭に、クラウドコンピューティングに対する取り組みを宣言した「オープンクラウドマニフェスト」が発表されました。また、利用者の立場に立ったベストプラクティスという意味で、「クラウドセキュリティアライアンス」が米国で立ち上がりました。これには富士通も参加しており、クラウドにおけるセキュリティのベストプラクティスの普及促進を目指しています。

技術に関しては、大学関係が中心の OCC（Open Cloud Consortium）が、さまざまな運用の標準化を行っています。また、DMTF（Distributed Management Task Force）という組織がオープンなクラウドリソ

ース管理についての検討会を設けました。そして、クラウドに技術的に一番関連する部のグリッドフォーラム OGF（Open Grid Forum）があります。

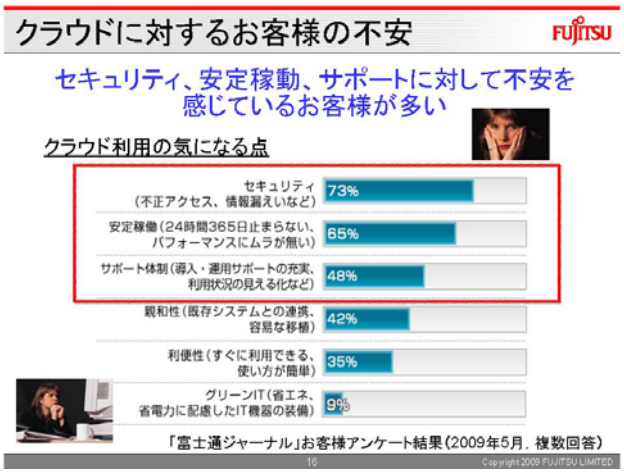
日本の国内では経済産業省が、「クラウドコンピューティングと日本の競争力に関する研究会」を立ち上げました。総務省でも、「スマート・クラウド研究会」を立ち上げました。クラウドセンター間の API（Application Program Interface）の標準化や、SLA などの保証レベルの検討や、著作権や個人情報などの扱いについて法律の検討も進んでいます。たとえば、ヨーロッパには個人情報処理に関する EU 指令があります。協定を結んでいるのは、ヨーロッパとアメリカで、日本は入っていませんが、クラウドコンピューティングを使ってグローバルなサービスを始めたいときに、個人情報や著作権を統一して扱うルールが必要になってきます（図表 4)。

（図表 4）クラウドコンピューティング政府・業界の動向

■クラウドの課題と不安

クラウドの課題については、大きく 4 つのことが挙げられています。
たとえば「信頼性の問題」。99.99%以上の稼働率を保証できるか、データの安全性は大丈夫かといったことですが、それらは、2 つ目の「セキュリティ」にも絡んできます。3 つ目に、「堅牢性の問題」。そして、4 つ目が「ロックイン」。ロックインとは、PaaS のようなミドルウェアまで用意されている環境では、そこの API に縛られてしまい、その開発環境でしか自分の作ったアプリケーションが動かないという、囲い込みのことです。

『富士通ジャーナル』(2009 年 5 月号）のアンケートでも、不安の第 1 位は、不正アクセスや情報漏えいといったセキュリティについて、続いて、安定稼働についてとなっています。例えば 99.99%といっても、約 52 分/年 以内の停止時間があるわけです。そして、パフォーマンスのムラについても心配されています。特に期末に処理が集中すると、CPU 負荷率が上がり、ネットワーク帯域もかなり占有されてきます。このようなリソースの使用状況やパフォーマンスなどの見える化、さらにトラブル時のＱ／Ａ対応やシステム回復時間などが心配の種になっています（図表 5)。



（図表 5）クラウドに対するお客様の不安

ある研究会が発足するときに、「複雑化するクラウド事業者間でのデータ管理基準は統一できるか？」「クラウド内での顧客データ同士の独立性は確保されるか？」「ユーザー間でのデータ取り違え等は発生しないか？」「クラウド全体がマルウェアの攻撃対象になるのでは？」といった指摘がありました。

さらに、クラウドのセキュリティリスクに関して言うと、サーバの特権ユーザー管理が、最大のセキュリティリスクです。J-SOX では IT 全般統制の監査も行うよう指導されており、その中の最も大きなポイントの 1 つに、サーバ特権管理があります。サーバ特権で何でもできてしまうということは、ログの改ざんやソフトウェアの入れ替えができてしまうということです。したがって、「特権ユーザーのアクセス管理」は、クラウドに限らず非常に重要です。

「コンプライアンスへの対応」も非常に複雑です。日本でセキュリティと言うと、個人情報保護法や不正アクセス対策法、J-SOX 法などがありますが、海外には非常に多くのコンプライアンス要求事項があります。例えば、米国では金融の個人情報では GLBA（Gramm-Leach-Bliley Act、金融サービス近代化法）、医療なら HIPPA、カードなら PCIDSS（Payment Card Industry Data Security Standard、クレジット業界におけるグローバルセキュリティ基準）があります。日本のセンターでそれらに対応できないと、海外のお客様が使えなくなってしまう心配があります。一方、それらに対応することになったとき、海外の法律を治外権として、日本国内で当てはめるようなことが本当にできるのかという議論もあります。

さらに、「データの保管場所」やユーザーごとの「データの分離」、「データのリカバリ」も問題です。Amazon の 3S（Simple Storage Services）は暗号鍵を使ってバックアップをとります。その暗号鍵を利用者がなくしても、Amazon はリカバリしてくれません。キーリカバリのシステムが備わっていないからですが、それは利用者責任ということで割り切らないと仕方ありません。ほかにも、「不適切・不正行為の調査」、「サービスの継続性」など、考慮しなければならない問題があります。

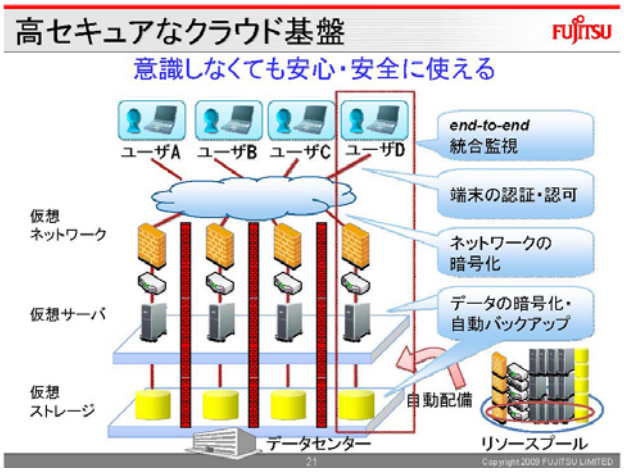
■クラウドのテクノロジー

クラウドのテクノロジーについては、富士通で来年オープンするクラウドセンターを例にとり、ご紹介

します。
クラウドの本質は、「仮想化」の技術を使ってハードウェア・ソフトウェアリソースをできるだけ最適にマネジメントし、利用していくことです。使うマシンのイメージを「標準化」して、セキュリティチェックしたものを提供すること。そして、運用プロセスに関する操作・手続きもできるだけ「自動化」していくことです。現在、この 3 つのコンセプトを基に開発を進めています（図表 6)。

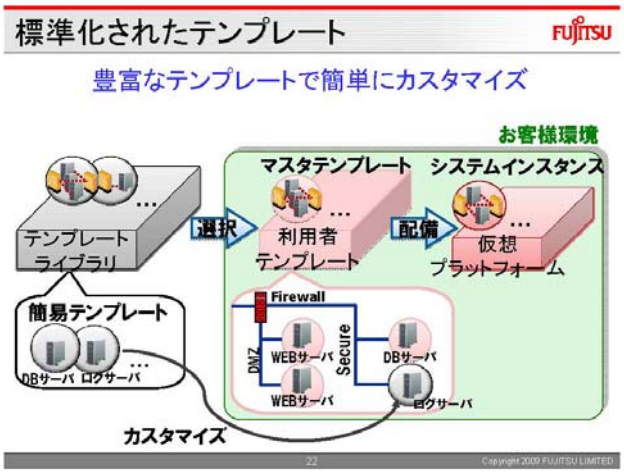
（図表 6）クラウドの本質

ご利用イメージとしては、end-to-end でクライアント環境からサーバ環境、アプリケーションサーバ、データサーバまですべてを監視する仕組みを入れ、端末には、三要素認証といって、端末認証や利用者認証・環境認証などの認証技術を入れます(FENICS でご提供します)。ネットワークは、利用者端末からクラウド環境まで、SSL-VPN で暗号化がなされています、ストレージも ETERNUS の中で自動的に暗号化されるような仕組みになっています。リソースプールでは、このようなサーバファーム、ストレージファームなどプールされた環境から、利用者のイメージを選択していただき、自動的に利用者領域に配置するということを行います（図表 7)。



（図表 7）高セキュアなクラウド基盤

マシンイメージは、すでに TRIOLE テンプレートとしてご提供していますが、それをクラウド環境の中で実現します。そこでは、ファイアーウォールやウェブサーバ、データベースサーバの組み合わせをテンプレート化し、カスタマイズのオプションを選択します。例えば、ログマネジメントのサーバの追加が必要であれば、それを追加することができます。リソースやサーバの利用状況は、ダッシュボードを用意して、できるだけ「見える化」するようにします（図表 8)。



（図表 8）標準化されたテンプレート

技術的な話になりますが、ストレージは ETERNUS の機能を使ってデータ暗号化を行います。図の仮想サーバの TPM（Trusted Platform Module）というのは、暗号技術を使って、各仮想サーバのシステムイメージのシグニチャをソフトウェア的に管理することを予定しています。そのシグネチャーと合わないものは動かさないという仕組みです。これにより、あらかじめ決められたテンプレートのシグネチャーと一致するものだけを配置し、動かすため、なりすましのソフトウェアが入らないのです。

また、経済産業省から支援をいただいたセキュアな環境を作るセキュアプラットフォームの技術を利用し各 VM（Virtual Machine、仮想マシン）の保護も行っています。ネットワークは、それぞれバーチャル LAN を張り、最終的にはファイアーウォールも、物理的なものから仮想的なものにして、各 VM すべてに入れることを計画しています。

館林の第 2 新棟にオープンした高セキュアな自動化されたデータセンターは、荒川の水害対策や地震、電力など、さまざまなことに考慮した最新鋭のセンターになっています。スーパーコンピュータによる冷却シミュレーションで、いかに冷却効率を高めるかといったことも行っています。ぜひご覧いただきたいと思います。

すでに富士通では、オンデマンド Linux や、オンデマンド Windows など個別のクラウド環境の構築サービス、運用サービスを提供していますが、現在のサービスはすべてのオペレーションを自動化するまでには至っておりません。しかし、来年にはクラウドマネージャーという、お客様と対話してリソースの選択、配置、稼働監視、課金まで行える環境をご提供したいと思っています。

■クラウドのセキュリティ

クラウドのセキュリティについては、2 つの視点があります。それは、「テクノロジー」の面と、「サービス保証」の面です。セキュリティのテクノロジーは、かなり成長してきており、認証でも、ID・パスワードのほか、ワンタイムパスワードや電子証明書を使うといった、利用形態に応じた認証技術があります。クラウドマネージャーも、最初は ID・パスワードですが、より機密性を要求される業務に強いワンタイムパスワードや電子証明書のようなオプションも用意したいと思っています。

暗号や鍵については、中のデータはお客様しか見えないように、ETERNUS が持っている暗号鍵と暗号技術を使ったストレージのサービスを提供していきますが、最終的にはお客様自身に暗号鍵を作成し、管理していただくというかたちになると思います。情報資産のオーナーはお客様自身ですから、お客様が責任を持って管理できる形態というのが望ましいと思っています。
仮想ネットワークは、スケーラビリティに対応可能なネットワークの保護など、サービスで開発していく技術が必要になると思います。仮想環境については、よりセキュアな VM の実現と特権管理をご提供していきたいと思います。ファイアーウォールや IDP（侵入検知遮断システム）は、アプライアンスとしての利用形態が多いと思いますが、最終的な形態を考えれば、仮想的なアプライアンスになっていくと考えられます。仮想的なアプライアンスとは、サーバファームも仮想になっていくように、アプライアンスもその空間ごとに配置できるようなソフトウェアプライアンス、バーチャルアプライアンスのことです。技術的にはまだこれからですが、富士通の目指すべきターゲットは、そのようなかたちだと思います。難しいのはマルウェアです。ウイルスがいないという保証だけではなく、お客様の作成されるアプリケーションの中にも不正なプログラムが入っていないという保証が求められます。特にソフトウェア開発環境などでご提供するとき、例えば、金利の端を落として集めるようなソフトウェアが、アプリケーションの中に紛れ込んでいないことを証明しなければなりません。いろいろなことを行うと、基本料金がどんどんアップしてしまうので、ある程度のスタンダードなラインとご要求に応じた内容を SLA で決めていくべきと考えています。

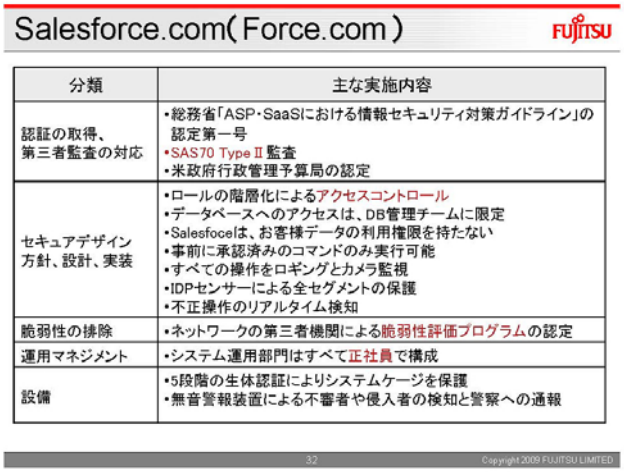
ここで視点を変えて、ホームページで公開されている Google、セールスフォース、Amazon EC2 のセキュリティポリシーを見てみたいと思います。統一的な書き方のガイドラインがないので、自由なフォーマットで書かれているものを、あえて同じ項目で比較してみました（図表 9）（図表 10）（図表 11）。

Google(Google Apps Premier Edition)

分類	主な実施内容
認証の取得、第三者監査の対応	•GLBA、HIPAA等政府プライバシー規制への対応 •ISO17799、GAAP、AICPA Trust Service、SAS70TypeⅡ対応
セキュアデザイン方針、設計、実装	•法的な拘束力を持つプライバシーポリシーの公開 •専門チームによるネットワーク境界等の防御、脆弱性検知 •不要なメッセージを送信しているサーバのトラッキング(PTIN) •シングルサインオンAPIの提供(SAML2.0準拠) •すべてのシステムへのアクセスを暗号化(SSH)
脆弱性の排除	•メールおよびWebアクセスのフィルタリング(ウイルス、スパム) •ネットワークやアプリケーションの脆弱性評価 •外部機関によるシステムとアプリケーションのセキュリティ評価 •ユーザーに影響する問題発生時のメールによる通知
運用マネジメント	•スタッフのユーザ環境へのアクセスを制限
設備	•外部および内部に監視カメラを設置、施設内への出入りを制限 •プライマリデータセンタに対し、セカンダリまたは補助データセンターを用意し、障害時には自動的に引き継ぎを実施

GLBA:金融機関向けの顧客情報秘密に関する米国の法律、　AICPA:米国公認会計士協会
HIPAA:米国の医療保険の相互運用と説明責任に関する法律、PTIN:Postini 社のThreat Identification Network

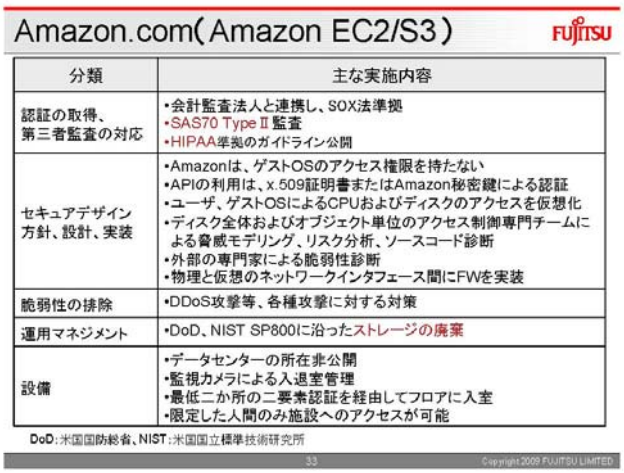
（図表 9）Google（Google Apps Premier Edition）



Salesforce.com(Force.com)

分類	主な実施内容
認証の取得、第三者監査の対応	•総務省「ASP・SaaSにおける情報セキュリティ対策ガイドライン」の認定第一号 •SAS70 TypeⅡ監査 •米政府行政管理予算局の認定
セキュアデザイン方針、設計、実装	•ロールの階層化によるアクセスコントロール •データベースへのアクセスは、DB管理チームに限定 •Salesforceは、お客様データの利用権限を持たない •事前に承認済みのコマンドのみ実行可能 •すべての操作をロギングとカメラ監視 •IDPセンサーによる全セグメントの保護 •不正操作のリアルタイム検知
脆弱性の排除	•ネットワークの第三者機関による脆弱性評価プログラムの認定
運用マネジメント	•システム運用部門はすべて正社員で構成
設備	•5段階の生体認証によりシステムケージを保護 •無音警報装置による不審者や侵入者の検知と警察への通報

（図表 10）Salesforce.com（Force.com）



Amazon.com(Amazon EC2/S3)

分類	主な実施内容
認証の取得、第三者監査の対応	•会計監査法人と連携し、SOX法準拠 •SAS70 TypeⅡ監査 •HIPAA準拠のガイドライン公開
セキュアデザイン方針、設計、実装	•Amazonは、ゲストOSのアクセス権限を持たない •APIの利用は、x.509証明書またはAmazon秘密鍵による認証 •ユーザ、ゲストOSによるCPUおよびディスクのアクセスを仮想化 •ディスク全体およびオブジェクト単位のアクセス制御専門チームによる脅威モデリング、リスク分析、ソースコード診断 •外部の専門家による脆弱性診断 •物理と仮想のネットワークインタフェース間にFWを実装
脆弱性の排除	•DDoS攻撃等、各種攻撃に対する対策
運用マネジメント	•DoD、NIST SP800に沿ったストレージの廃棄
設備	•データセンターの所在非公開 •監視カメラによる入退室管理 •最低二か所の二要素認証を経由してフロアに入室 •限定した人間のみ施設へのアクセスが可能

DoD:米国国防総省、NIST:米国国立標準技術研究所

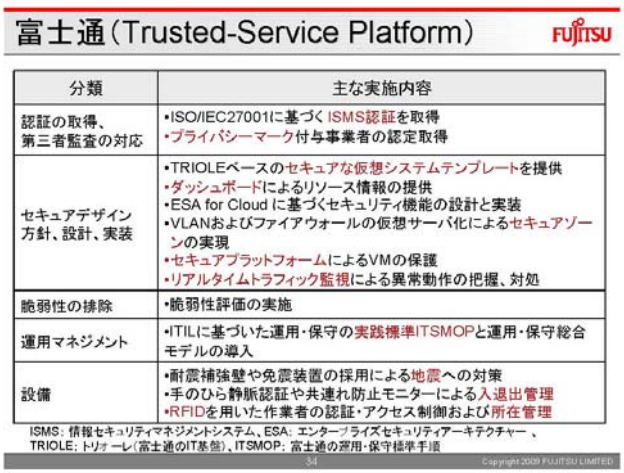
（図表 11）Amazon.com（Amazon EC2/S3）

Google では、EU 指令 25 条でヨーロッパから勝手に個人情報を持ち出してはならないということもあり、プライバシーには非常に神経を使っていることがわかります。各種プライバシー規程にも対応していま

す。各社それぞれ ISO の ISMS（情報セキュリティマネジメントシステム）に代表される ISO17799（情報セキュリティ管理のガイドライン）に対応しており、海外は特に SAS70（Statement on Auditing Standards 70、米国 SOX 法に対応した情報セキュリティ統制の監査基準）の認証を受けたり、Amazon では、HIPPA の医療ガイドラインがうたわれています。全体的に概略のポリシーという体裁で、抽象的であり、セキュアデザインや方針、設計などは、あまり細かく書かれておりません。内部にセキュリティの専門チームがいて検証をしているなどが書かれています。また SAML2.0（Security Assertion Markup Language、ID やパスワードの認証情報交換のための XML 仕様）はシングルサインオンをするような環境をきちんと出すといったことが書いてあります。Google ではウイルスやスパム対策については、非常によくやっているようです。

セールスフォースは、実際書いてあるレベルはあまり詳しくありませんが、あるお客さまの 300 項目くらいのセキュリティ要求事項に対して、290 以上応えられたと言われています。対応できなかったのは FISC（The Center for Financial Industry Information Systems、金融情報システムセンター）の細かい基準ですが、あまり使われないものなので、ほとんど影響はないと思われます。

富士通でも、国内で必要な認証関係や、テンプレートの安全化、ダッシュボードによる見える化など、コアとなるバーチャリゼーションのセキュア化といったものに対応していきますし、脆弱性や運用の標準化、フィジカルな面も中に入れていく予定です（図表 12）。


富士通（Trusted-Service Platform）

分類	主な実施内容
認証の取得、第三者監査の対応	•ISO/IEC27001に基づくISMS認証を取得 •プライバシーマーク付与事業者の認定取得
セキュアデザイン方針、設計、実装	•TRIOLEベースのセキュアな仮想システムテンプレートを提供 •ダッシュボードによるリソース情報の提供 •ESA for Cloud に基づくセキュリティ機能の設計と実装 •VLANおよびファイアウォールの仮想サーバ化によるセキュアゾーンの実現 •セキュアプラットフォームによるVMの保護 •リアルタイムトラフィック監視による異常動作の把握、対処
脆弱性の排除	•脆弱性評価の実施
運用マネジメント	•ITILに基づいた運用・保守の実践標準ITSMOPと運用・保守総合モデルの導入
設備	•耐震補強壁や免震装置の採用による地震への対策 •手のひら静脈認証や共連れ防止モニターによる入退出管理 •RFIDを用いた作業者の認証・アクセス制御および所在管理

ISMS：情報セキュリティマネジメントシステム、ESA：エンタープライズセキュリティアーキテクチャー 、
TRIOLE：トリオーレ（富士通のIT基盤）、ITSMOP：富士通の運用・保守標準手順

（図表 12）富士通（Trusted-Service Platform）

各センターのセキュリティ情報の開示は、どの程度まで開示してよいか基準がありません。まだ各社で周りも見ながら少しずつ公開されているようです。政府の委員会でも、内容についてある程度項目の標準化を決めて、SLA 案のようなものを出して、各社それぞれベンチマークができるようなかたちにしていこうという方向に動いています。年内は無理かもしれませんが、来年には、ある程度の分類項目が標準化され、各社のサービス状況が比較できるようになってくると思われます。

今、富士通が予定している可視化は、「リソース稼働状況の可視化」や、不正アクセスの状況など「セキュリティ状況の可視化」、「利用アプリケーション価値の可視化」、「アプリケーション稼働資産の可視

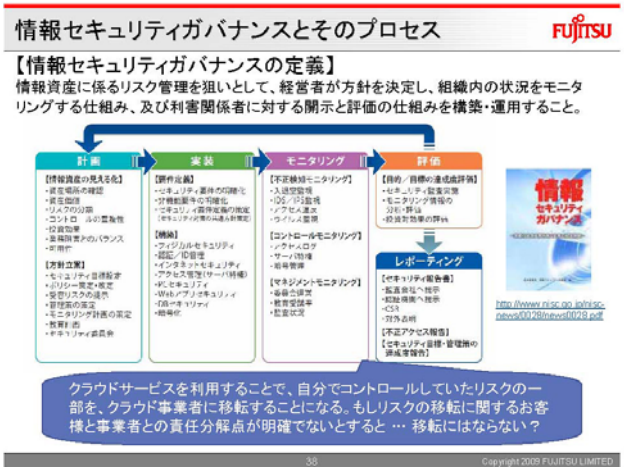
化」などです。まだデザインが統一されていないのですが、できるだけ同じようなデザインにするような方向で進めていきます。

別の観点から、リスクと適用形態のお話をします。米国 NIST からの資料ですが、リスクを考える上で、一番脅威にさらされているセンターはインターネット上に公開されているパブリッククラウドだと思われます。反対に、自分の中に作る、一部の利用者で利用するプライベートクラウドは、最も脅威が少ないと考えられます。しかし、プライベートクラウドは色々な業務要件が要求されます。そこには非常に細かなセキュリティ要求事項が入ってきます。そうした状況においてクラウド事業者は、一意のセキュリティアーキテクチャーを実装すると思われますが、パブリックだけではすべての要求は対応できないので、プライベートクラウド的なものをそのセンターの中に作っていかざるを得ません。プライベートクラウドのほうが、セキュリティの要求事項としてはより細かくなっていくと思われます。

中小企業の IT 促進には、経済産業省の SaaS 事業の適用もありますが、IT を持つことから利用する方向へ促され、パブリック SaaS や、パブリッククラウドの利用が進んでいくと思われます。大企業はプライベートクラウドを開発し、さらにクラウド間でハイブリッドクラウド化されていくのではないかと思われます。

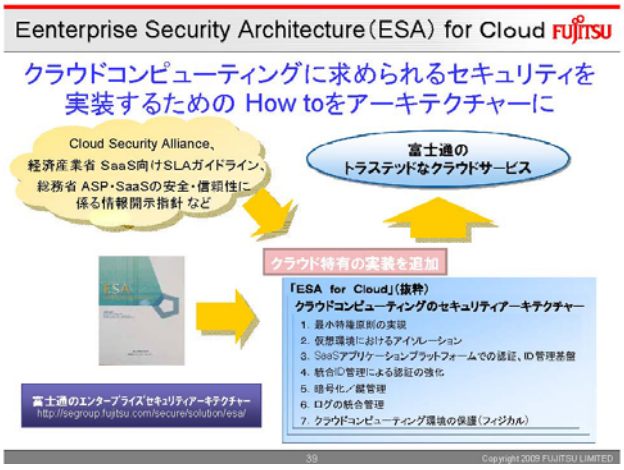
■情報セキュリティガバナンス

このような中で、クラウドのサービスにおいても、情報セキュリティに対しての目標を持ち、そのセキュリティ目標がきちんと達成できているかということを可視化して評価するような仕組み、いわゆる情報セキュリティガバナンスという考えが重要です。
政府から『情報セキュリティガバナンス』という本が刊行されています。この本には、企業のトップは情報セキュリティに対してリスクを意識し、受容できるリスクとできないリスク、受容できないものに対しては、きちんと計画フェーズから関与して、その対策がとれていることを評価する仕組みを作ること、その評価する仕組みの中には監査役も入り、経営トップも関与しなければならないことが書いてあります。これは、クラウドにおいてもまったく同じ要求事項です（図表 13)。



（図表 13）情報セキュリティガバナンスとそのプロセス

クラウドサービスを利用することで、今まで自社のセンターで自らがコントロールしていたリスクの一部を、クラウド事業者に渡すことになります。しかし、移転したと自分で思っていても、クラウド事業者はそう思っていないケースもあるかも知れません。PaaS であれば OS、ミドルまでは PaaS 事業者が面倒を見るけれども、その上位アプリケーションは利用者側の問題として割り切られることもあるでしょう。責任分解点を明確にするべきだと弁護士や公認会計士の方々がお話しされています。
1 つの事例を申し上げれば、今年から J-SOX 法で、IT 全般統制を検査するように言われていますが、クラウド事業者のセンターの中の IT 全般統制は検査できるのか、証拠となるようなログやエビデンスというのはクラウド事業者が出すのか、ユーザーが出すのかといったことが問題になっています。
パブリッククラウドでは、提供できるポリシーというのはそれほど細かなものではありません。一意のポリシーで、業務共通に利用すると思います。そこには ID・パスワードによる認証やファイアーウォールによるインターネットのアクセスコントロール暗号通信の利用などの項目が入ってくると思われますが、これだけでは当然セキュリティポリシーが足りないということになれば、より細かな認証や業務ごとのアクセスコントロール、ログなどが要求されると思われます。
また内部統制では、よく言われているように、開発と運用は分けるべきで、開発用のクラウドと運用用のクラウドは、別々のアクセスポリシーで作るべきであり、そうした証跡を監査会社から求められることが予想されます。
富士通でも、クラウドにおけるセキュリティの必要要件に関して「ESA for Cloud」という名前で、ホームページで公開の予定です。クラウドのサービスを支えるためのコンサル系のサービスや監視系のサービスを用意していきたいと思っています（図表 14)。



（図表 14）Enterprise Security Architecture (ESA) for Cloud

私どものセンターでは、クラウドの運用部門とセキュリティ監視部門を分けています。運用部門が自分でログを管理・監査するのではなく、クラウドセキュリティセンターという別部門がその運用状況やログの中身を見ます。独立性をもって証跡として監査会社に出せるようなかたちにするため、このように分けて運用することを考えています。またクラウドセキュリティセンターは私どものクラウドセンターほか関連会社のセンターの監視も行い、お客様のプライベートクラウドや他社のクラウドセンターのログ管理とその分析やレポートについてもサービスをご提供するかたちを考えています。

2009 年の 4 月 2 日、アメリカ・テキサスのデータセンター（Core IP Networks LLC）が、FBI から予告なしにデータセンターのシャットダウン命令を受けました。その後すべての機材が令状によって押収され同社の顧客 50 社が電子メールやデータベースのアクセスログを失いました。FBI は押収した理由について、同社から過去にサービスを購入したことのある企業を調査するためと説明しました。そうなると、私どもクラウド事業者も、コンプライアンスや法律を意識しなければなりませんし、必要なときにはきちんとデータや証跡が出せるような仕組みを作っていかないといけません。フォレンジックでは、データ自身も、警察が要求してくるのは、ビットバイナリでコピーしたものです。ビットバイナリのコピーでないと、法的には通用しないこともあるので、そうした設備もゆくゆくは日本でも必要になってきます。また海外法人業務を請け負うためには、ある程度その国のルールも考慮しておく必要があります。

クラウド提供者は、お客様の ICT の効率的な利用価値だけではなく、サービス形態に対しても、きちんとセキュリティ要件を明確に提示する必要があります。そして、利用者の方々も、こうしたことをきちんと理解した上で契約をしなければなりません。

以上でプレゼンテーションを終わります。ご清聴ありがとうございました。