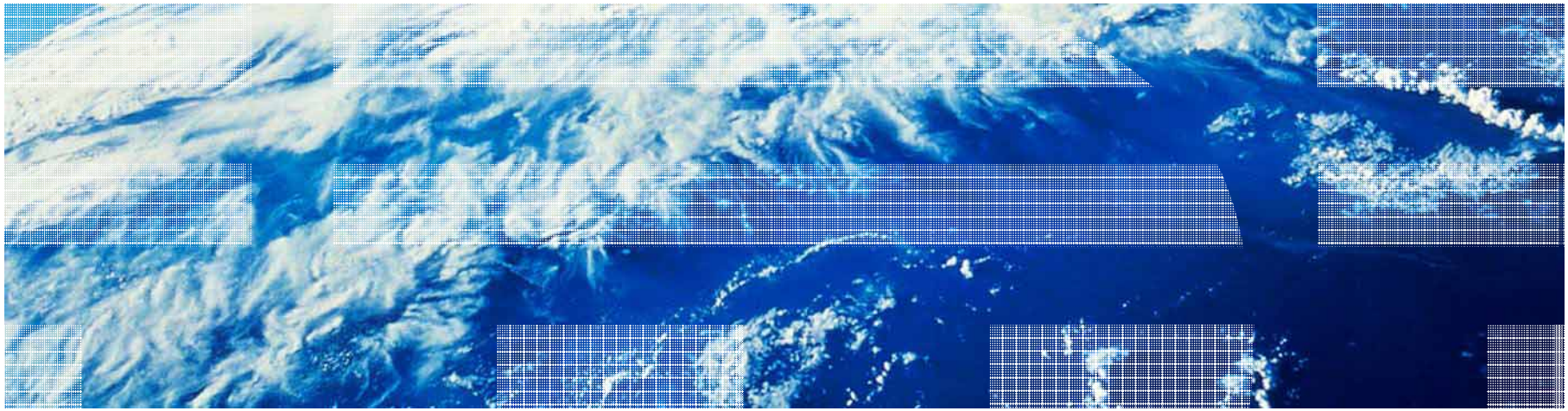
2010年2月20日
情報セキュリティの日「第4回JSSMセキュリティ公開討論会」

クラウドコンピューティングにおける セキュリティ問題に関する考察

日本アイ・ビー・エム株式会社 東京基礎研究所
吉濱 佐知子



概要

- クラウドコンピューティングが生まれた背景
- 定義や形態
- クラウドにおけるセキュリティ課題
- クラウドにおけるセキュリティ対策
- まとめ

クラウドコンピューティングが生まれた背景

- ITシステムは年々複雑さを増しています
  - 情報爆発の影響で、ストレージ領域が年54%ずつ増加
  - ITコストの70%は既存機器の管理やメンテナンス費用
  - IT資源の85%は使用されていない
- 過去十数年に渡る企業のIT投資額を分析すると
  - 新規購入費用は横ばい
  - トランザクション増加により、サーバ台数は飛躍的に増大
    - 運用管理費も飛躍的に増大し、ITコストの大部分を占める
    - これに伴ない、電源・空調関連費用も増大
- 運用・管理コストの削減はCIOの課題
  → クラウド・コンピューティングにより、運用・管理コストの削減が期待されている

ビジネスとしてのクラウドコンピューティング

- IT各社が、クラウドコンピューティングに投資を開始している

- クラウドの適用分野例
  - 解析
  - コラボレーション
  - 開発・テスト
  - デスクトップ
  - インフラストラクチャ
  - ビジネスサービス

- お客様の要求に合わせた柔軟な構成

IBM、専門組織の設立など本年度のクラウド事業への取り組みを発表

3 users　ブログ転載　2010/01/15

IBM　クラウド

- 【リユースサーバを活用したITコスト削減を提案】システム延命支援
- 【新製品情報】シマンテックから低価格バックアップソフトが新登場！
- サイコムの省電力PC[Silent-Master] 静音派から熱い支持！
- 【Windows7】無償アップグレードキャンペーン対象製品

日本アイ・ビー・エムは1月14日、クラウドコンピューティング事業に関する記者説明会を開催した。同社は1月1日付けで社長直属のクラウド統括組織を設立するとともに、新たにクラウドの最高技術責任者(CTO:Chief Technical Officer)を任命し、クラウドビジネスを推進するチームを結成するなど、積極的にクラウドビジネスを進めていく構えだ。

クラウド・コンピューティング事業を統括する執行役員の吉崎敏文氏は、企業向けクラウドにおける同社の強みとして、「技術面でのリーダーシップ」、「ソリューション・ポートフォリオ」、「豊富なクラウド導入実績」、「グローバルにわたる英知とスケールメリット」の4点を挙げた。

同氏はこれらのうち、技術面でのリー

マイコミジャーナル (01/15)
http://journal.mycom.co.jp/news/2010/01/15/009/?rt=na

国家戦略としてのクラウドコンピューティング

- 米国
  - オバマ大統領によるOpen Government Directiveの提唱
  - Vivek Kundra 氏を連邦CIOに任命 (Mar 2009)
  - 連邦政府の保持するデータを公開するdata.gov の創設 (May 2009)
  - 行政向けクラウドサービスカタログApps.gov公開 (Sep 2009)

GSA Apps.Gov A Service Provided by GSA

Cloud "G-Cloud"

26/06/2009

Government Cloud

I have started taking part in a
posted this item to answer a

- 英国
  - 英国CIOのJohn Suffolk氏のCloud Strategy発表 (June 2009)
    - Standardize, Rationalize, and Simplify
    - “G-Cloud” in UK
    - Government Application Store ("G-AS“)

クラウドコンピューティングの定義や形態

クラウドコンピューティングの定義 (1)

米国国立標準技術研究所 (NIST) における定義

- **オンデマンド・セルフサービス(On-demand self-service)**
  - ユーザが必要に応じて、自分でプロビジョニングを行えること。(サービス提供者側の人間を介する必要がない)
- **広いネットワークアクセス (Broad network access)**
  - 機能がネットワーク上で提供される
  - 標準的な仕組みを使って多様なクライアント・プラットフォームからアクセスできる
- **リソースの確保と割り当て (Resource pooling)**
  - サービス提供者の計算資源が、複数の顧客に対してマルチテナントモデルで提供されるように確保されており、顧客のニーズに従って物理的・仮想的な資源が動的に割り当てられること。
- **迅速な弾性 (Rapid elasticity)**
  - 計算資源の量をすばやく柔軟に調節できる
  - 顧客が必要なだけの計算資源をほぼ無尽蔵に購入できる
- **利用状況の計測と報告 (Measured Service)**
  - クラウド提供者が資源の利用状況を計測し、制御・最適化する
  - 資源の利用状況が利用者と提供者に報告されること。

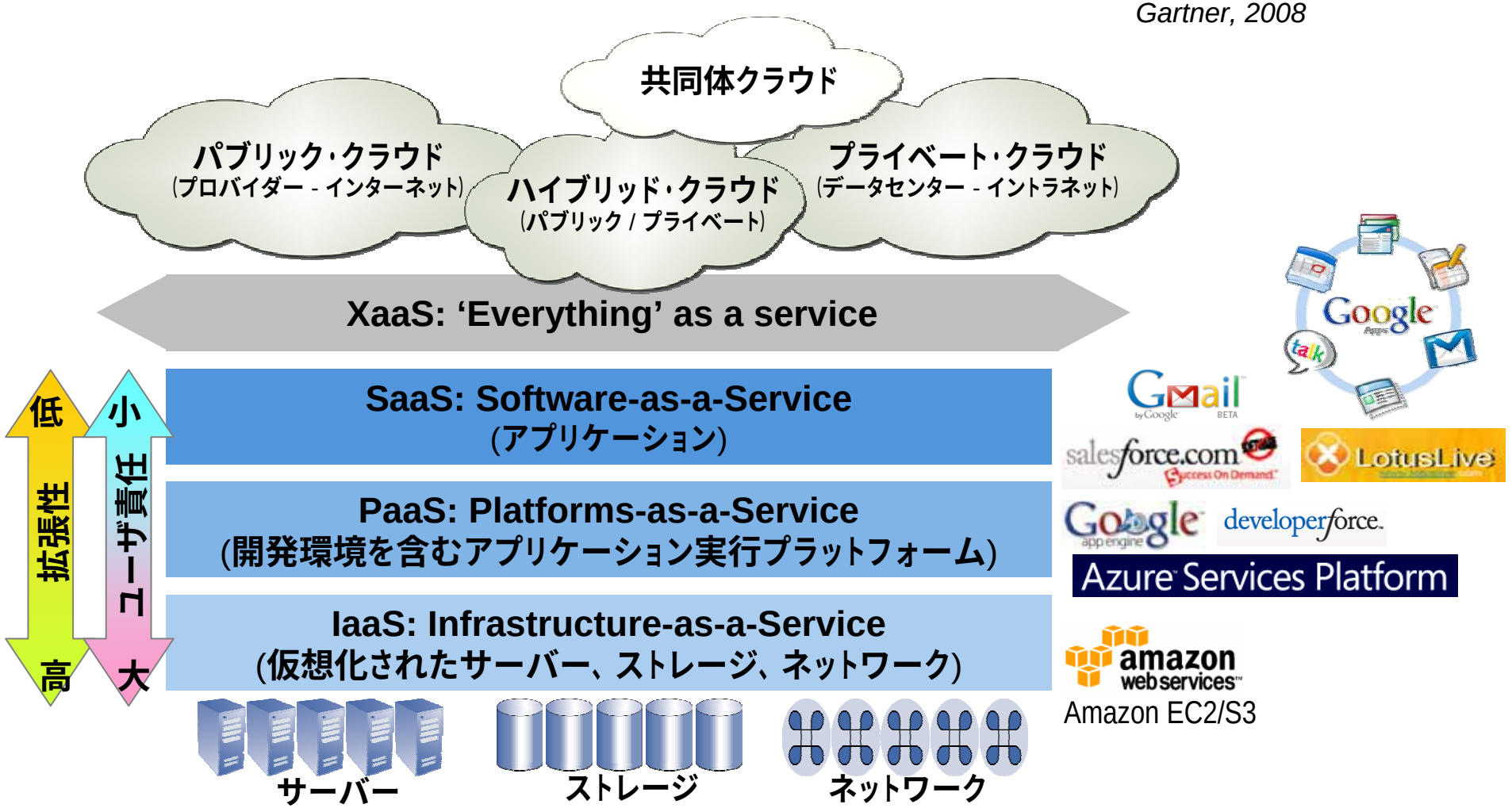
Source: If applicable, describe source origin

*出典: http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

クラウド・コンピューティングの定義 (2)

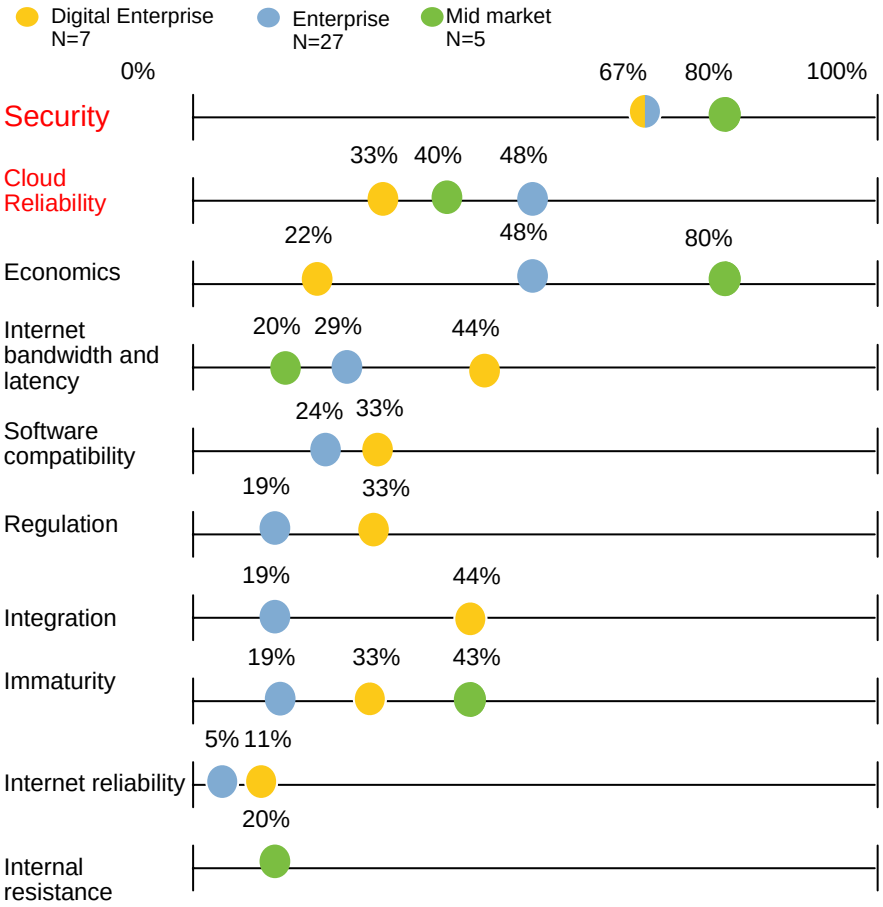
a style of computing where massively scalable IT-related capabilities are provided 'as a service' across the Internet to multiple external customers

Gartner, 2008



課題

セキュリティは、クラウドコンピューティングにおける主要なリスクだと考えられています

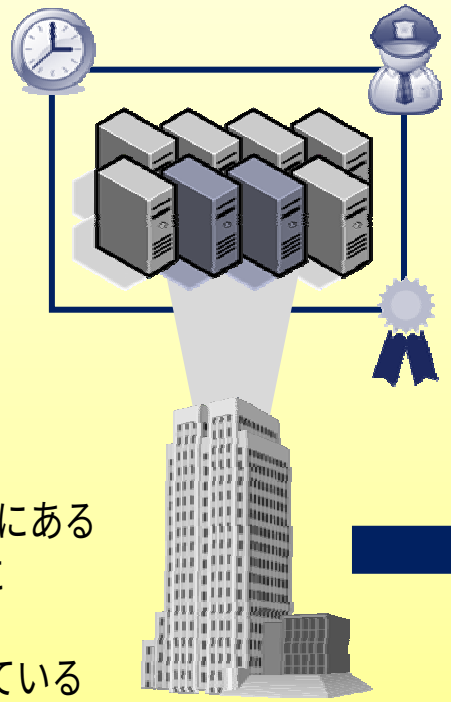


Source: Oliver Wyman Interviews

- セキュリティは、通常、新しいITソリューションに対する懸念としてしばしばトップにあげられますが、外部に置かれるクラウド環境では、より深刻な問題です
- 顧客は、特にクラウドコンピューティングにおけるデータセキュリティと実際の信頼性に関して懸念を感じています
- 大企業は、外部的なソリューションよりもエンタープライズ・クラウドがよりセキュアであると考えています

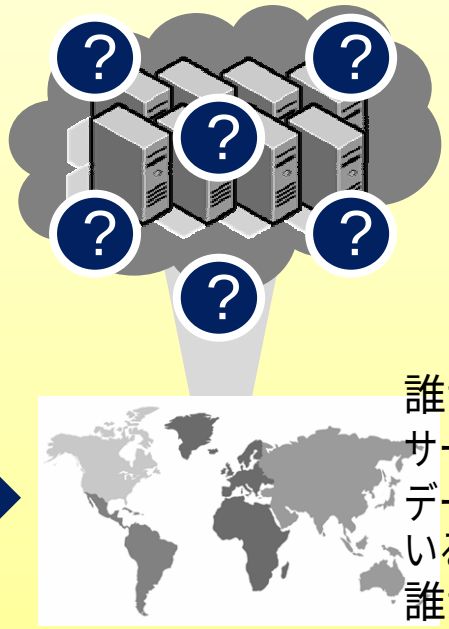
クラウドセキュリティの基礎

TODAY



自社で管理されている
サーバーはXという場所にある
データはサーバーY, Zに
保管されている
適切にバックアップされている
管理者がアクセス権を管理している
稼働時間は十分である
監査がきちんとなされている.
自社のセキュリティチームが関与している

TOMORROW



誰が管理するのか？
サーバーはどこにあるのか？
データはどこに保管されて
いるか？
誰がバックアップを取るのか?
誰がアクセス権を持っているか?
弾力性はあるか?
どのように監査するのか?
どのように自社のセキュリティ
チームが関与するのか？

クラウド環境におけるセキュリティーの懸念事項 (1)
ポリシーや組織に関するリスク

- ガバナンスの欠如
- データやサービスの移行困難 (ロックイン)
  - クラウド提供者を変更したり、自社システムに戻ったりするのが困難になる
- コンプライアンス
  - 業界標準や法律で定められた認証を受けられるか
    - 例：PCI DSSにおける立入検査要件
- 他のユーザの風評被害
- クラウド提供者が営業停止する
- クラウド提供者が買収される
- クラウド提供者の内部犯行者
- クラウド提供者の業務委託先での問題
- 顧客とクラウド提供者の責任範囲が不明瞭

クラウド環境におけるセキュリティーの懸念事項 (2)
法的リスク

- 裁判所命令によるハードウェア没収や電子証拠開示
- 司法管轄 (国境等) の問題
- データ保護法への違反
- ソフトウェア使用規約違反

データ保護、プライバシーに関する各国の動き

- 米国
  - 米国愛国者法 (PATRIOT Act)
    - 電話やEメール、医療情報、金融情報や他の記録について政府が調査する権限を拡大　-> 保管された企業データが米政府に公開される危険性
  - 米国企業改革法 (SOX法)
  - Payment Card Industry Data Security Standard (PCI-DSS)
    - ペイメントカード情報セキュリティの国際統一基準
  - 医療保険の相互運用性と説明責任に関する法律 (Health Insurance Portability and Accountability Act：HIPAA)
    - 個人を特定することのできる医療データを、患者の同意なしに第三者機関に開示することを制限
- EU
  - 個人データ保護指令
    - 個人データの処理に係る個人の保護及びその自由な流通に関する欧州議会及びＥＵ理事会指令（９５／４６／ＥＣ）
    - 個人データの第三国への移転は、その国が十分なレベルの保護措置を確保している場合に限って行うことができる ->データベースの暗号化などが必要
  - データ保護指令を受け、EU各国でデータ保護法の施行
    - 米国とEUはセーフハーバー協定を締結

クラウド環境におけるセキュリティーの懸念事項 (3)
技術的リスク

- 実行環境分離が不十分
  - 異なるユーザの使用する計算機資源 (仮想マシンやストレージ等) の分離が不十分な場合にセキュリティ的な問題が発生する危険がある。
- 仮想マシンモニタ等クラウド管理機構への攻撃
  - 脆弱性があれば大きな被害を受ける可能性がある。
  - Webの管理インタフェースなどは脆弱性の発生リスクが高い
- データ保護
  - クラウド提供者がどのようなデータ保護を実施しているかについて十分な情報が得られないことが多い
  - 不完全なデータ削除
- アイデンティティ管理
  - 自社システムとクラウド、複数クラウド間でのアイデンティティ統合

Crime as a Service (aka Dark Cloud, Crime Cloud, etc.)

- 容易に計算機資源を入手できるクラウド環境が、攻撃のためのプラットフォームとなる危険性 (ラック社のレポートより)
  http://www.itmedia.co.jp/enterprise/articles/0912/08/news062.html
  - Amazon AWSのドメインによる攻撃: 2009年11月末で約250件
  - ボット用のサーバをGoogleのAppEngine上に構築
  - Amazon EC2でパスワードの総当たり攻撃
    - アルファベット8文字を使うパスワード: 3ドル
    - 数字を含めた場合: 45ドル程度で成功
- パブリッククラウド上での攻撃の危険性
  Amazon EC2上でのサイドチャネル攻撃の試行
  - “You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,”, by Thomas Ristenpart, et. al., ACM CCS 2009.
  - VMインスタンスが、どこに配置されるかを知ることができるか?
  - 2つのインスタンスが同じ物理マシンに置かれていることを検知できるか?
  - 攻撃用VMを、攻撃対象のインスタンスと同じマシン上に置くことができるか？
  - VMをまたがって情報を盗み出すことができるか?

対策

クラウド環境におけるセキュリティー上のメリット

- 高いレベルのセキュリティサービスを実現
  - セキュリティ技術がクラウドベンダに集約される
  - クラウド提供者にとってはセキュリティが差別化要因
- 脆弱性対策などへの素早い対応
  - 脆弱性の情報収集や分析に規模の効果
- 遠隔地であることのメリット
  - 災害時のリカバリが容易に
- 迅速なスケールイン／アウトによる弾性
  - DDoS (分散サービス拒否) 攻撃への耐性
- 仮想化技術によりフォレンジック分析が容易に
- 計算機資源が集約されることで、物理的セキュリティの向上が容易になる

→ 信頼できるクラウド提供者を選択すれば、セキュリティ上のメリットは大きい

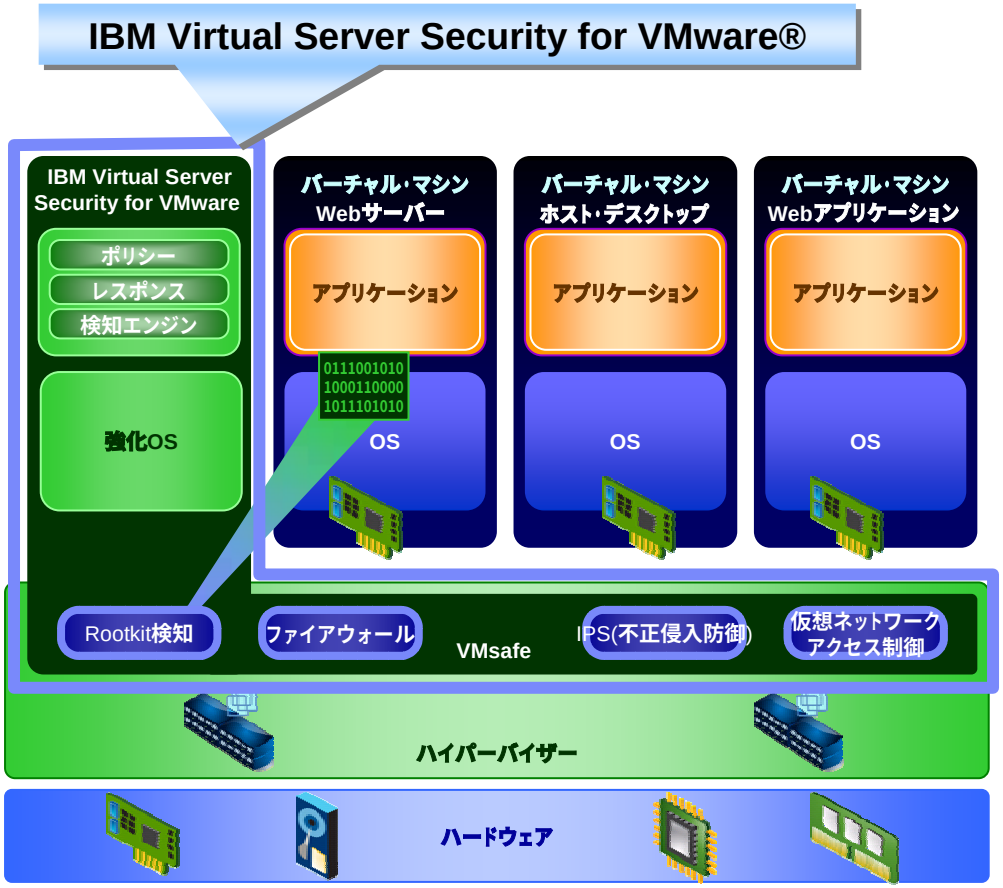
IBMセキュリティー・フレームワークにおけるソリューション例

セキュリティーエリア	対策	IBM ソリューション例	
アイデンティティー管理 	ID・権限管理、セキュリティーポリシー管理、セキュリティー教育	■ Tivoli Identity Manager ■ Tivoli Access Manager for e-business ■ Tivoli Federated Identity Manager	■ IBM Tivoli Access Manager for Operating Systems ■ IBM ISS Education Service
データ保護、情報管理 	コンテンツ・セキュリティー、暗号化、ログ管理、アクセス制御	■ IBM Fidelis XPS ■ IBM クライアント・セキュリティー・ソリューション ■ IBM ISS Proventia Network Mail Security ■ IBM Optim	■ IBM Eメール・セキュリティー管理サービス ■ IBM Tivoli Security Information and Event Manager ■ IBM WebSphere DataPower ■ IBM エンド・ポイント暗号化支援
アプリケーション・プロセス 	アクセス制御、脆弱性監査、ポリシー管理	■ IBM ISS Webセキュリティー診断サービス ■ IBM Rational AppScan ■ IBM Tivoli Security Policy Manager	■ IBM Tivoli Access Manager for Enterprise Single Sign-On ■ Tivoli Access Manager for e-business
ネットワーク・サーバー・エンドポイント 	アクセス制御、不正侵入防御、ウィルス対策、脆弱性監査	■ IBM ISS Proventia Network Enterprise Scanner ■ IBM ISS Proventia Network IPS ■ IBM ISS Proventia Network Virtual IPS	■ IBM ISS Proventia Server ■ IBM ISS Proventia Network Multi-Function Security ■ IBM ISS インフラ・セキュリティー診断サービス ■ Virtual Server Security for VMware (VSS)
物理インフラストラクチャー 	入退室管理、遠隔セキュリティー監視、ビデオ監視	■ IBM IB-ACCESS ■ IBM Managed Security Services	■ IBM Smart Surveillance Solution

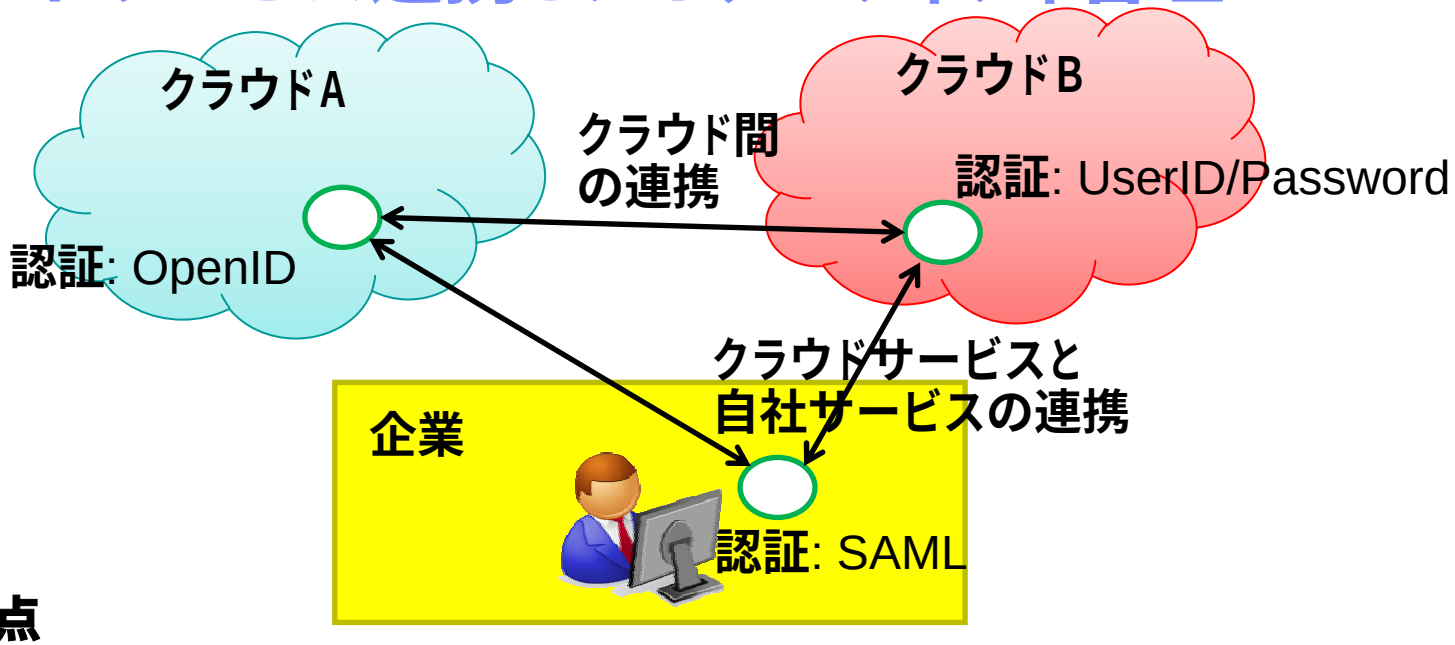
IBM Virtual Server Security for VMware (VSS)の発表

VSSはVMware VMsafe™ APIを通して特権レベルでハイパーバイザーと連携し、仮想化環境全体のセキュリティーを保護

1. **X-Force Virtual Patch技術を仮想ネットワークに適用**
   - VM間通信の保護、外部からVMに対する通信の保護
2. **ハイパーバイザの乗っ取り防止技術**
   - **ハイパーバイザ　アンチルートキット**
     by X-Force & IBM Research
3. **仮想環境におけるコンプライアンスの準拠**
   - VM自動ディスカバリ、 仮想ネットワークアクセス制御 (vNAC) 、仮想環境内の監査
4. **仮想リソースの負荷軽減と仮想化セキュリティの両立**
   - ゲストOSにはAgent不用、1つのVSSで仮想環境全ての脅威を保護



クラウドサービス連携とアイデンティティ管理



- **問題点**
  - アイデンティの表現や交換プロトコルが統一されていない
    - UserID/Password, OpenID, SAML, etc.
  - 認証・認可のためのポリシー管理の実装ががまちまち
- **取り組み**
  - 製品でのサポート (例. IBM Tivoli Federated Identity Manager)
  - コミュニティ・標準化
    - Kantara Initiative (アイデンティティ管理技術の普及を目指すOpen Community)
    - OASIS Identity in the Clouds TC

Web アプリケーションセキュリティ

Web 2.0 ・ SaaS アプリケーションを保護するための エンド・ツー・エンドのセキュリティ技術開発

課題

- Web 2.0やマッシュアップ アプリケーションに対する攻撃への対策
- SaaS環境でのビジネスデータの保護

東京基礎研究所の技術

- コンテンツフィルタリング技術 (ACF: Active Content Filter)
  - 様々なコンテンツタイプへの攻撃を防御 (JSON, RSS/Atom, Flash …)
  - 異常検知技術により、悪意のある入力データを判別
- セキュア・マッシュアップ (SMash)
  - 既存のブラウザ上でマッシュアップされたコンテンツを分離し、安全に実行するためのフレームワーク
- ドキュメント情報漏えい防止技術
  - ドキュメントの内容から機密度を判断

コンテンツ・フィルタ

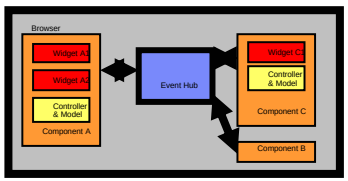
悪意のあるコンテンツの サニタイゼーション

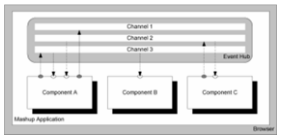
情報漏えい防止

SaaS環境でのビジネスデータの保護 とコンプライアンス

安全なマッシュアップ技術

異なる信頼度を持つプロバイダのサービスを 安全に統合する





Security as a Service:
クラウドサービスとしてのセキュリティ

- “Security as a service refers to the practice of delivering traditional security applications as an Internet-based service, on-demand, to consumers and businesses.” (Wikipedia)
- Managed Security Serviceと違い、自社の管理者にポリシー設定などのコントロールがある
- Security as a Serviceの例
  - Anti-* suite
  - 脆弱性分析
  - ログ管理
  - アセット管理

IBM Rational AppScan OnDemand

どのクラウド提供者を信頼すればいいのか？

- ASP・SaaS安全・信頼性に係る情報開示認定
  - マルチメディア振興センター http://www.fmmc.or.jp/asp-nintei/
  - 総務省「「ＡＳＰ・ＳａａＳの安全・信頼性に係る情報開示指針」*1 に基づく
  - 安全・信頼性に関わる実施水準や状態に関する情報がASP・SaaSのサービスを提供する事業者から適切に開示されていることを認定
  - 安全・信頼性に関わる実施水準や状態そのものを認定するものではない

- 第三者機関による認定
  - ISMS認定
  - SAS 70 -- 内部統制の監査基準（SOX法404条に対応）
    - クラウド提供者が内部統制状態を証明する手段として注目

- SLA (サービスレベル合意) による確認
  - 経済産業省「SaaS 向け SLA ガイドライン」*2 による確認項目例
    - ISO/IEC 27001 に対応したセキュリティ対策の実施状況、
    - 脆弱性検査、安全性検証試験／セキュリティ診断の実施と結果の公開
    - データベース管理、データのダウンロードやバックアップ可否
    - アカウント管理、アクセス制御、通信の暗号化
    - ログ管理・提供、保守管理計画、サポート時間、最大サービス停止時間
    - コンプライアンス対応、利用者に対する情報セキュリティ監査の受け入れ、保険への加入

*1 http://www.soumu.go.jp/menu_news/s-news/2007/071127_3.html
*2 http://www.meti.go.jp/press/20080121004/20080121004.html

まとめ

- “Cloud Security is a tractable problem”
  - NIST: Presentation on Effectively and Securely Using the Cloud Computing Paradigm v26
    - http://csrc.nist.gov/groups/SNS/cloud-computing/

- セキュリティ上のリスクとメリットについての正しい理解が必要
  - 必要なセキュリティ要件を満たせる提供者を選択
  - 契約やSLAの締結
  - 必要に応じてプライベート・クラウドとパブリック・クラウドを使い分け、これらを統合するハイブリッド・クラウドが今後の傾向

ご静聴ありがとうございました