クラウドコンピューティングとIT統制
境を越えるIT統制　共通規範への取組

The IT Contorol for Cloud Computing

Grapple to make Common **Rules**

清水　惠子
（公認会計士、システム監査技術者、ITコーディネータ）

201012.11(富山賞受賞記念講演会)

目次

1. クラウドのIT統制の課題
2. 現状の懸念事項
3. クラウドコンピューティング発展に向けて求められるもの
4. 制度面
5. 技術面
6. 外部委託先監査の動向
7. まとめ

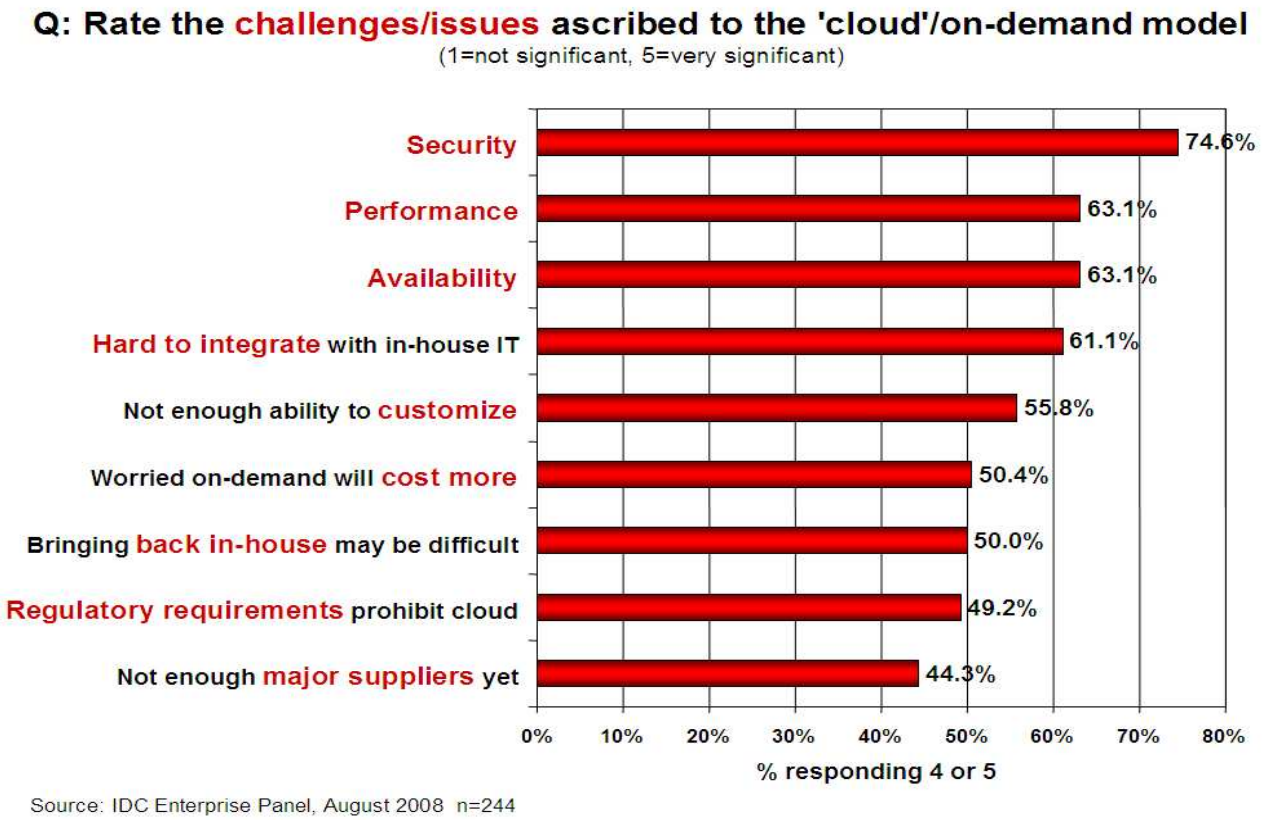
1. クラウドのIT統制の課題

- ユーザはITを利用するが所有しない
  - 特約を結ばないとデータの保管場所は指定できないのが通常
  - システム構成やセンターの場所は通常は開示されない
  - ユーザは通常、直接にはIT統制を確認できない
- IT統制は、ベンダーに依存する
  - パブリッククラウドのIT統制は一般的な条項によるため、ユーザの要件を満たすとは限らない
  - ベンダーの責任範囲とユーザの責任範囲が明確でない場合がある
  - 個人情報や機密情報についての取扱は国毎に異なる
- ユーザは利用する責任を負うか
  - 委託元の管理責任（内部統制制度）（実施基準Ⅱ2（1）②6）

2. クラウドコンピューティングの懸念事項

- やはり、懸念はセキュリティ

図表2：NISTから転載



3クラウドの発展に向けて求められるもの

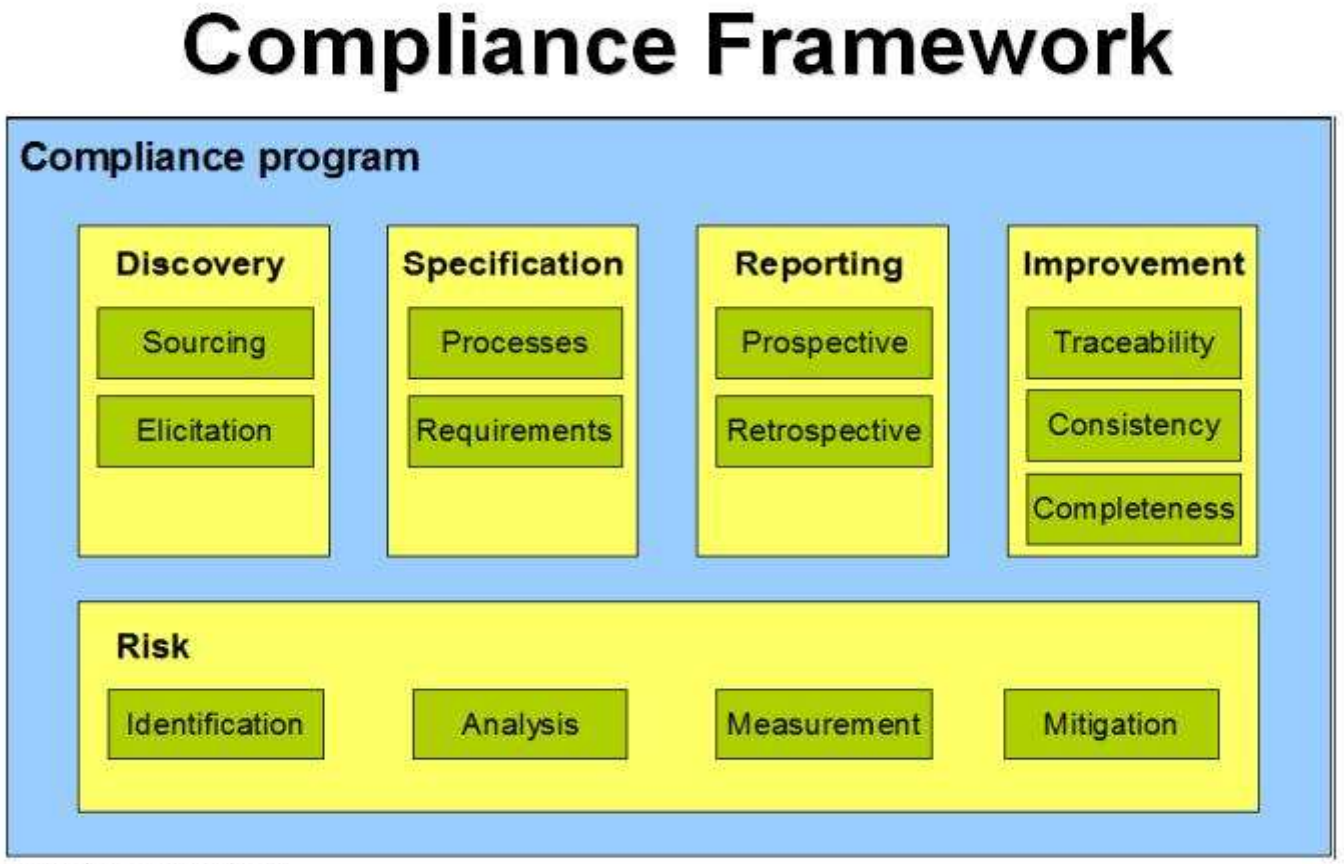
ITに対する統制は、各国の国情により、差異があり、EU指令など個人情報のデータ移転についての統制にも国により対応に差がある。国境を越えてのITの利用を促進するには、一定の安定したルールが求められる。統制は、法令などの制度面と技術面での統制の強化がある。統制は、標準化された技術等で互換性を高めたり、セキュリティの強化など安定した、また、安全なIT環境を提供する反面、利便性の低下やコスト増、自由な競争を妨げる面の両面を兼ね備えている。

一定の規制（法律や基準）が国際的に確立しても、各国の組織、特に各企業のITシステムが、法の要求を満たすように構築されることや、運用しているITシステムが確かに、法の要求を満たしていることを、検証するのは容易なことではない。

4制度面①
コンプライアンスフレームワーク

- コンプライアンス：フレームワーク
  - 法令工学（Law-Compliance）
    - 米国では、法律の条文を論理的に分解して、関係者の権利や義務を明らかにして行く　研究が行われ、医療情報保護法（HIPPA：Health Insurance Portability and　Accountability Act）などで、事例研究が進められている。
    - EUにおいても、法制度の異なるEU諸国に対して、単一のEU指令を発して、諸国間の　統制を維持するために、コンプライアンス・フレームワークの研究、構築が進められ いる。
    - 法律や基準は、一度施行されると、環境の変化などに迅速に対応させるのは、　難しいため、ある程度幅を持たせた表現を取ることが多い

4制度面②
コンプライアンス・フレームワーク



COMPAS Project
（Compliance-driven Models, Languages, and Architectures for Services）
State-of-the-art in the field of compliance languages

4制度面③
サイバー空間の安全確保

- 国際電気通信連合（ITU）（元は万国電信連合）は国際間の電気通信（無線通信も含む）の標準化や規制を確立する目的の国際機関。
- 「サイバースペースには国境がなく、各国が共有できる空間、リソースである。国境を越えたサイバー犯罪に対しては国際間の協力が必要である。」とし、そのために国際協定、Cyber Treatyが提唱されており、CoEの条約などをもとにToolkitを公表している。ToolKitにはサイバー犯罪のモデル協定が含まれている。
- サイバー空間は、海、陸地、大気、宇宙空間に続いて第５番目の共通空間であり、サイバー空間の安全の確保にはサイバーセキュリティとサイバー犯罪を含むサイバー協定が必要である（ Norway のJudge Stein Schjolberg の国連でのプレゼンテーション（論文2010/4/13）
- クラウドにおいては、複数の国のまたがり、複数の司法管轄にかかわる犯罪の懸念があり、サイバー空間協定を通して手続法の世界的な協調が図られる必要がある。
- 郵便制度のように、安定した制度になれるか？

4制度面
個人情報保護

- 個人情報についてはEU指令があるが、個人データの国際案移転とデータ処理に関するプライバシー保護の国際標準の動き（個人データ・プライバシーコミッショナー会議）国際標準案が策定されている。この草案は、国際的に受け入れられる最高レベル」を目指している。
- 従来の個人情報保護の課題と今後の要請
  - 事業者にとっては複雑すぎる：データを扱う責任者としてのベンダーにとってシンプルの要請
  - 個人情報保護には不十分との認識：個人にとって熱い保護の要請
  - 特定のベンダーや特定の国に有利なルールではなく、広く、コンセンサスを得ることが重要となる。
- 各国によって個人データの扱いには、差がある。必要な保護と自由なデータ移転のバランスが課題となる

5技術面①
NGN≪次世代ネットワーク≫

- 次世代ネットワーク（NGN）とは
  - 信頼性、安全性の面で従来の電話網が持つ技術やノウハウを活用しつつ、IP網の柔軟性・経済性を盛り込んだ次世代の情報通信ネットワーク
  - これまでのIP網が、利用料の面でベストエフォート型の利用を中心に利用者の支持を得たのに対し、ベストエフォートのクラスも維持しつつ「品質確保クラス」を付加して、リアルタイム性が必要な利用者への要求を満たす目的がある。
- キャリアの課題と現状
  - これまでのPSTN（公衆回線網（固定電話の回線網））の利用者をNGNに収容して、旧設備を廃棄し、通信インフラや端末の維持費削減を早急に実現する必要があり、それを優先する企業も多いため、直ちに利用者に全面解放されない場合もあるが、公衆回線網のIT化として、重要な発展である。
  - 欧米（米国、英国、フランス、ドイツ、イタリア、オランダ等）や東アジア（日本、韓国、中国、台湾、香港、シンガポール等）の2地域では、インフラ構築への取組みが進んでいるが、この2地域以外では、次世代網への移行はゆっくりとした変革に留まり、世界中がNGNに足並みを揃えるのは、相当先のこととなるであろう。
  - インタフェースの公開が行なわれると、他のキャリアやサービス事業者のサービス創成を容易化すべく、「NGNアプリケーション用アダプタ」が市場投入されたり、応用開発のために独自の利用法が様々の業界で進むため、ネットワークの世界に国境が形成されたりする。
  - 各国が自国の状況に合わせてNGN化を進めて行くと、世界のNGN技術の標準化が遅延し、国毎のインフラを国毎の法律で律する体制ができ上がる。標準化が成った後、技術的に足並みが揃っても、各国の法律が障害となり、クラウドが国際間で最適利用される可能性が阻害される。従って、早期に、国際条約などで国別の法律運用の齟齬を予防する努力が必要になる。

5技術面②
Swarm Computing

- Swarm Computingとは多くのコンピューティングデバイスに囲まれた状況の中で、人間がどのようにそれを利用するかというコンセプトである。
  - 今日「ネットワーク」と呼ばれるものは、PCのネットワークではなく、もはやモバイルデバイスのネットワークである
  - 内在するセキュリティ問題に対処するためには、最下層レイヤーと最上位のレイヤーでコントロールを実現していく
- 2010年3月RSA会議
  - 目標は、「クラウド環境を構成するハードウェアの信頼性を保証する基盤（root of trust）」を確立し、プライベート・クラウド内に、共通する物理特性や同一のセキュリティ・ポリシーを共有するためのリソース・プールを用意すること
- 仮想環境でのハードウェアと仮想レイヤの情報を収集し、セキュリティ情報とイベント管理を利用して分析・評価することにより、クラウドコンピューティングのベースレイヤーでの透過性を高めつつ、安全と規制順守対策をとることができるとしている。
-

6外部委託先の監査

12

- 既存の監査制度
  - ISMS
  - SAS70
  - 18号
  - クラウド監査用？（AICPA）
  - 経済産業省の公開草案
    - クラウドセキュリティガイドライン

図表4CSA（Cloud Security Alliance）のSecurityガイドライン

Domain 4: Compliance and Audit

・Cloud Provider's SAS 70 Type II. Providers should have this audit statement at a minimum, as it will provide a recognizable point of reference for auditors and assessors. Since a SAS 70 Type II audit only assures that controls are implemented as documented, it is equally important to understand the scope of the SAS 70 audit, and whether these controls meet your requirements.

・ Cloud Provider's ISO/IEC 27001/27002 Roadmap. Cloud providers seeking to provide mission critical services should embrace the ISO/IEC 27001 standard for information security management systems. If the provider has not achieved ISO/IEC 27001 certification, they should demonstrate alignment with ISO 27002 practices.

・ISO/IEC 27001/27002 Scoping. The Cloud Security Alliance is issuing an industry call to action to align cloud providers behind the ISO/IEC 27001 certification, to assure that scoping does not omit critical certification criteria.

7まとめ

- 技術面でも、制度面でも世界的に安定したルールが求められている
  - 各国の事情があり、完全に同じルールでは運用できない
  - 技術面でもシステム構成等により、実現方法は全く同じではない
- ルールの策定については目指す方向性が重要
  - 日本としての自主的な主張（受動的ではなく能動的）
  - ルール運営の柔軟性（法は全ての事実を網羅できない）
- 日本から世界への積極的な発信

IT研究会
WG3メンバー紹介

グループリーダ
　清水　恵子
メンバー
　澤田　栄浩
　田吹　隆明
　河本　高文
　和田　康

清水恵子（（株）日本ブレインウエアトラスト　）

公認会計士、システム監査技術者、ISMS（ISO27001）主任審査員
会計不正検査士、ITコーディネータ、CGEIT

大手監査法人で会計監査の主査を務めた後、ITアドバイザリー部門でシステム監査、情報セキュリティ監査に従事した。
EAガイドラインの策定、システム管理基準の改定、追補版の策定にも関与した。
現在はITコンサルティング会社でビジネス戦略部長、未来技術研究所長

日本公認会計士協会　：
　監査IT対応専門委員会委員
　ITアシュアランス専門委員会
経済産業省：
　情報セキュリティガバナンス研究会情報セキュリティ報告書モデルWG 2007年
　プロテクションプロファイルの利活用に関する調査研究　委員会委員 2008年
　システム管理基準改定に向けた検討会　委員会委員 2008年
　クラウドセキュリティ検討委員会委員2009年
東京都：
　システム評価委員会
この他にも、政府等の委員会委員を務める