Vol.2012-IS-119 No.15
2012/3/16

工科系単科大学へのクラウドコンピューティング適用検討

石坂　徹†，刀川　真†，石田　純一†

クラウドコンピューティングが情報システムのコストダウン，セキュリティに対する要求を満たすための手法として注目されている．大学でもクラウドコンピューティングによる様々なサービスの展開が進められているが，企業に比べ特に学務や経営など事務処理系では進んでいるとは言えない．これは企業と大学組織の体質，文化の差異によるものと考えられる．クラウドコンピューティング適用のためには，まず方式と特徴を理解するとともに，大学の組織特性を把握する必要がある．これに基づいて，業務おける問題点と心理的阻害要因を分析し，工科系単科大学を例として大学業務のクラウドコンピューティング適用の課題と対応策を検討する．

Consideration of Cloud Computing in Engineering College

Tohru ISHIZAKA†, Makoto TACHIKAWA
and Jun-ichi ISHIDA†

Cloud computing is paid attentions as to meet requirements for the cost cut and security of information systems. Although various services by cloud computing is promoted at the university, works of secretariat, such as school affairs and management, are not progressed compared with company. This is considered to be based on the difference of the nature between a company and a university. In order to apply cloud computing, understanding a system and the feature first, it is necessary to grasp the organization characteristic of a university. Based on this consideration, we analyze the problem in works and mental prevention factors to reject of cloud computing. Furthermore, assignments and countermeasures of cloud computing application of university business is considered by making an engineering college into an example.

† 室蘭工業大学
Muroran Institute of Technology

1. はじめに

情報システムの新たな実現法として，クラウドコンピューティング（以下クラウド）が広がりを見せており，大学等の高等教育機関でも今後，クラウドの広範な利用が想定される．しかし企業等とは組織の体質や文化が異なるため，そこでの導入例をそのまま活かせるとは限らず，また従来とは異なる問題の発生も考えられる．

そこで工科系単科大学を事例にし，大学の組織特性とクラウドの適合性を分析し，その導入の課題と対応策を探る．特に大学では，情報セキュリティのなかでも個人情報保護に関わる機密性保持が重要視される傾向にある．しかしその個別要因については必ずしも具体的な分析がなされてないため，リスクの存在が明確には認識されてないにもかかわらず不安が先立ち，結果的にクラウド導入が進んでない状況も散見する．そのため，併せて情報セキュリティ上の不安分析と，その対処策も提案する．

2. クラウドの方式と特徴

2.1 クラウドの本質的特徴

クラウドには幾つかの方式があり，利用形態等により分類される．ここでは，NIST(National Institute of Standards and Technology)による定義方法を用いる．

NIST による定義[1]では，クラウドは以下の本質的特徴をもつ．

On-Demand self-service:利用者が人を介することなく自動的にコンピュータの能力を使用することができる．

Broad network access: コンピュータの機能をネットワークを通じて，携帯電話，タブレット，ラップトップ，ワークステーションなど様々なクライアントから利用することができる．

Resource pooling: コンピューティング･リソースは利用する多数の利用者に共有，提供される．そこでは，利用者からの需要に応じて物理的あるいは仮想的なリソースが動的に割当／解消される．一般的に，そこで供給されるリソースの正確な位置を，顧客が制御したり知ることはない．

Rapid elasticity: コンピュータの機能は迅速にかつ順応的に供給され，場合に応じて自動的に，スケールアウトの際に拡大し，スケールインの際に縮小する．利用者にとって，この能力は無限に追加できるものになり，いつでも必要な分だけ購入することができる．

Measured Service. サービスの種類（ストレージ，プロセッサ，帯域，アクティブ･ユーザ･アカウント）に適した測定機能により，自動的にリソース利用を制御し，最適化

する．こうしたリソースの使用量は，利用されたサービスに対して，プロバイダーと契約者の双方からから，透過的にモニター，制御，レポートされる．

2.2 サービスモデル

サービスモデルによる分類では利用者に対して供与するリソースに応じて分類している．表 1 にサービスモデルの分類を示す

表 1　サービスモデルによる分類

サービスモデル	サービス形態
Cloud Software as a Service(SaaS):	アプリケーションがサービスとして提供される形態をいう．契約者はハードウェア及びアプリケーションを含めた管理や制御は行わない.
Cloud Platform as a Service (PaaS)	プロバイダーが提供する基盤に，契約者がアプリケーションを配置することができるサービス.
Cloud Infrastructure as a Service (IaaS)	主として仮想化されたサーバ基盤（仮想マシン）が提供されるサービス．契約者は任意の仮想マシン上で任意の OS，アプリケーションを動作させることができる.

2.3 展開モデル

展開モデルはだれがどこにサーバを置くかによって，分類したものである．表 2 に NIST の展開モデルによる分類を示す.

表 2　展開モデルによる分類

展開モデル	運用形態	設置場所
プライベートクラウド	特定の組織のために単独で運用される. 当該組織またはサード･パーティーにより管理される.	現地または遠隔地
コミュニティクラウド	複数の組織により共有され，関心事（事業，セキュリティ要件，ポリシー，コンプライアンス）を共有する特定のコミュニティをサポートする.	現地または遠隔地
パブリッククラウド	このクラウド･インフラストラクチャは，不特定多数の人々や大規模な業界団体などに提供される. 基盤の運用はサービス事業者である.	遠隔地
ハイブリッドクラウド	上記モデルの組み合わせ	現地または遠隔地

クラウド導入事例では，パブリッククラウドとプライベートクラウドを併用したハイブリッドクラウドで運用しているケースも多く見受けられる．これは情報及び情報システムを組織建屋内／外あるいは自組織管理／業者管理の棲み分けを行い，適切な場所にシステムを配置した結果である．特にセキュリティの観点から，情報システムの運用に関する知識・技術を持った情報センター等に集約したプライベートクラウドが構築されている．一般に情報システムを導入する場合，機密性の高い情報を扱う場合は管理者以外が立ち入りできない安全区域に設置することでセキュリティを維持する必要がある．さらにセキュリティとしては，可用性及び完全性も考量する必要があり,災害等に備えた非常用電源や防火対策,耐震対策など物理的な対策も必要である．業者のデータセンターではこれらの設備が整っており，自前で同等の対策を行うためには膨大なコストがかかることが予測される．一方学外のプライベートクラウドを構築する場合，ネットワークの可用性を重視し一般のネットワークとは別に大学とデータセンターの間を専用線で結ぶ，あるいは学外接続を多重化する，帯域を大きくするなどの措置が必要となる．これは仮想デスクトップ環境をクラウド化した DaaS(Desktop as a Service)など，即応性が求められるシステムを利用する場合には重視される.

3. 情報システムから見た工科系単科大学の組織特性

情報システムの導入は対象組織の特性を正確に認識しないと，十分な効果は期待できない．そこで情報システムの視点を中心にして工科系単科大学の組織特性を示す.

3.1 教員の自律性

大学教員は一般企業と異なり各個人の予算を持っており，各自の裁量によって執行することができる. 特にインターネットが各大学に接続され始めた 1990 年代後半には,コンピュータの知識をもつ教員が研究費で導入した UNIX ワークステーションや，PC でメールサーバや Web サーバを独自に立ち上げることがよく行われた．現在，メールや Web が大学として完備されているにも関わらず，この独自サーバを利用し続けることにより，セキュリティ上問題が発生することが懸念されている.

3.2 大学によるシステムの内製傾向

PC の低価格化と Java(TM)や軽量なスクリプト言語の浸透により，個人に配分された研究費でのシステム構築が安価・容易になった．これにより，教員の研究費で様々なシステム開発が行われ，大学の業務システムも研究の一つとして開発された.

一方，事務システムの情報化は，ミニコンを用いた会計システムから始まり，専用

クライアントとサーバによるネットワークシステムを経て，近年の Web 上のリッチクライアントへと変遷してきた[2]．その過程において前述の教員開発による大学内製システムも実際に業務に使用されてきた．これらの利用は工科系の中でも情報系学科を持つ大学でよく行われていたと思われる．この形態は教員としては研究の実績となり，大学としては高価なシステムを購入せずに開発・導入・保守を教員に行ってもらうことでコストダウンできるという，双方に対してのメリットがあると考えられた．しかしながら，この内製システムの利用はいくつかの問題をはらんでいる．その中の典型的な例としてシステムのメンテナンスの問題が挙げられる．システムは経年によりいずれは陳腐化し，またはバグなどの不具合も発生することが考えられる．しかし開発した教員がシステムのメンテナンスを行えば，大学としてはメンテナンス費用を少なく済ませられるかもしれないが，その分教員の本来の業務である教育・研究の稼働が減ることは考えられていない．この作業が研究と直結すれば双方のメリットとなるが，研究として新規性がないことが多く現実的ではない．

3.3 学内組織特性の均一性

単科大学では総合大学と比較すると学部間の特色や独自性を考慮することがないため，個別システムではなく全学で利用できる共通システムを導入することができる．また，教職員の数も少ないため情報系センターなどのスタッフにより，ほとんどすべての教職員に対して全学的に一様なサポートを行うことができる．

4. クラウド適用の課題

4.1 業務内容による課題

大学の主たる業務としては，教育，研究，地域貢献が挙げられる．これらの業務を支援するのが事務サービスであり，以下では事務システムに限定し，クラウドを適用した場合の効果を検討する．

4.1.1 経営系システム

経営系システムとしては，人事システム，給与・会計システム，財務システムなどが挙げられる．これらは主に経営層及び事務系職員が用いるシステムであり，一般的に個人情報，経営情報などの機密性が高い情報を扱うシステムといえる．この機密性の観点からすると，パブリッククラウドの利用やアウトソーシングなどによる外部組織の活用は敬遠されがちである．しかしながら，データの重要性（完全性，可用性）の観点からみると，クラウド環境への移行は堅牢なデータセンターの活用することを考えると十分に効果があると考えられる．

クラウドサービスの形態としては，市販のソフトウェアもクラウド化しているものもあり，今後充実が期待される SaaS が有効であると考えられる．大学固有の業務内容などにアプリケーションのカスタマイズ等が頻発する場合には，PaaS を用いることになるが，この場合，ソフトウェアの管理コストが嵩むことが考えられる．

展開モデルとしては SaaS を用いる場合はパブリッククラウドとなる．また，PaaS を用いる場合は，パブリックまたはプライベートの双方の形態が考えられるが，機密性を重視する場合はプライベートクラウドを選択することになるであろう．

4.1.2 学務系システム

学務系システムとして，学生の履修情報などの教務管理や就職情報管理，電子掲示板（デジタルサイネージ），入試情報管理など多種多様である．これらのシステムの運用においても個人情報保護は重要なセキュリティ要求事項である．静岡大学の事例[3]ではこれらのシステムは学外のデータセンターを用いたプライベートクラウドを用いている．複数キャンパスがある場合，データセンターの集約化という意味で有効であり，また，地震災害が懸念される静岡という立地を考えた場合，建物の堅牢性を重視したセキュリティ対策は重要である．一方，キャンパスが一つの単科大学を考えた場合，集約という意味は比較的弱くなるが，クラウド化全般に言えるハードウェアの管理コストの低減は大きな意義を持つ．特に学務系システムでは常時コンピューティングパワーを必要するようなことは少なく，繁忙期など限られた期間のみコンピュータリソースを増大させるなど，動的なリソース割り当てができるクラウド環境が適合すると考えられる．

4.1.3 基幹ネットワークサービス

様々な情報システムが大学業務で使用されるようになると，利用者がそれぞれのシステムの ID を管理することの煩雑さが生まれた．さらに，パスワードを紙や PC に記憶させるなどセキュリティ上好ましくない管理の仕方も発生することになった．最近，一つの ID で複数のシステムの認証を行う統合認証システムが多くの組織で用いられている．認証を行う認証サーバは複数のシステムからの認証要求を受け付けるため，最も頻繁にアクセスがあるサーバである．したがって，ネットワーク上で可用性が求められ，ID 及びパスワードという各システムを利用するうえで重要な情報を扱うという点で機密性の高いサーバともいえる．すでにクラウド利用を行っている多くの大学では前述の学務系システムと併せて，この認証サーバを学内外のプライベートクラウドに設置している．

教職員の電子メールや Web スペースも今や情報システム利用における基幹サービスといえる．これらのサービスは，すでに多くの大学が SaaS あるいは PaaS によって学外のクラウドサービスを利用している．基本的に個人が利用するサービスでは，最

近では学内のメールを Gmail など個人向けクラウドサービスや携帯電話に転送している利用者も多く，データ連携や機密性をそれほど必要としないため，もっとも早期にアウトソーシングされたサービスである．また，大学広報としての Web サービスは本来学外向けであり，災害や学内ネットワークトラブル発生時などでも広報できる体制が必要である．こういった観点からすると，Web サービスは学内に置くべきではなく，むしろ積極的に学外のクラウド環境を利用する必要があると考える．

5. クラウド化に対する心理的阻害要因の分析

5.1 クラウド化に伴うリスク分析

クラウド化の進展に伴いリスク分析も重要になっている．たとえば経済産業省の報告書[4]では，情報の安全性や信頼性に関するリスクや，データセンターを利用する場合に他社に関する捜査の影響を受けて自らのシステムが停止に陥るリスクなどに言及している．あるいは総務省の報告書[5]では，BCP(Business Continuity Plan)の策定などの重要性について述べている．しかしいずれもリスクを体系的に扱っているものではない．これに対し EU では，ネットワークセキュリティ及び情報セキュリティに関する予防・対応能力を促進することを任務とした ENISA（European Network and Information Security Agency：欧州 ネットワーク情報セキュリティ庁）が，クラウドのリスクを体系化している[6]．

ところでリスクとは，一般的には「ある行動に伴って（あるいは行動しないことによって），危険に遭う可能性や損をする可能性を意味する概念」 と理解されている[7]．しかし，リスクの要素（原因，対象など）は明確でないものの「不安」が先立ち，導入を躊躇することも考えなければならない．これに関して情報処理推進機構ではクラウドの導入事例とユーザ側の意識・懸念材料を調査・整理している[8]．また服部ら[9]は ENISA の体系に基づき国内の企業，行政機関，大学などに対してアンケートを行い，クラウドに対する利用者の意識調査をまとめている．調査対象が“意識”ということは回答が利用者の感覚に大きく左右されるものであり，これから「不安」が類推されると考える．

5.2 大学のクラウド化に伴う情報セキュリティの不安

大学の情報化は，企業などと較べてアウトソースが必ずしも進んでいるわけではないため，パブリッククラウドに象徴されるようにデータ設置や情報処理を地理的・組織的に大学の外部で行うことに対する抵抗感や不安感は，特に情報セキュリティに関してより大きいと考えられる．

情報セキュリティの 3 要素である機密性・完全性・可用性のうち，金融機関に代表されるようにわずかなデータの欠損や一瞬のサービス途絶も許されないサービスと比べ，大学にとっての完全性や可用性は相対的には制限が緩いと考えられる．しかし機密性については，中でも受験者や学生の成績や健康情報など個人情報に関するものについては漏えいが大学の評判低下に直結するため，大学にとっても企業等と同等かそれ以上に神経を使う要素であろう．

そこで服部ら[9]の成果を元に ENISA のリスク分類のうち機密性に関する部分を抽出し，それらに対する服部らによる利用者の意識調査結果と大学がクラウド化した場合の推定危険度を表 3 に示す．なお危険度の推定に際しては，以下の前提を置く．もちろんこれらの前提は個々の大学や事業者に依るものであり一律には断定できないものの，感覚的には共感を得るものと考える．

＜前提＞
クラウドサービス提供事業者の方が大学より優れていると考えられるもの
　α：IT 設備等の堅牢さ（ハードウェア，ソフトウェア）
　β：建物などファシリティの充実
　γ：運用管理の厳格性
クラウドサービス提供事業者の方が大学より劣ると考えられるもの
　δ：担当者の顧客（大学）に対するロイヤリティ
その他
　ε：アウトソースすることにより新たな危険発生があり得る

表 3　大学クラウド化に対する機密性に関するリスク分析

＜技術的リスク＞

項番	リスク要因	ENISA 評価	利用者の不安意識	クラウド化推定危険度 (　)：根拠
A	CLOUD PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES 事業者の内部者によるセキュリティ違反（不正アクセスなど）で自組織の機密情報が見られその事実が分からないリスク	High	≒40%	＋ (δ)
B	MANAGEMENT INTERFACE COMPROMISE 事業者が意図的に，自組織の機密情報を盗み見するリスク	Medium	≒26%	＋ (δ)

C	INTERCEPTING DATA IN TRANSIT DATA LEAKAGE ON UP/DOWNLOAD, INTRACLOUD 事業者へのデータ転送の際に機密情報が漏えいするリスク	Medium	≒21%	＋ (ε)
D	INSECURE OR INEFFECTIVE DELETION OF DATA 事業者が不要になったデータを消去しないリスク	Medium	≒18%	－ (γ)
E	UNDERTAKING MALICIOUS PROBES OR SCANS スキャン（空いているポートを探すなど）のリスク	Medium	≒9%	－ (γ)

＜共通的リスク＞

F	PRIVILEGE ESCALATION 事業者のルート権限を奪取されて，自組織情報が盗まれたり，改ざんされるリスク	Medium	≒27%	－ (γ)
G	SOCIAL ENGINEERING ATTACKS 事業者がソーシャルエンジニアリング攻撃を受けて，自組織に関する情報を開示するリスク	Medium	≒21%	± (α)
H	LOSS OR COMPROMISE OF OPERATIONAL LOGS 自組織サービスが取得しているログを紛失したり，漏えいさせるリスク	Low	≒18%	－ (γ)
I	LOSS OR COMPROMISE OF SECURITY LOGS 事業者が認証などのセキュリティログを紛失したり，漏えいさせるリスク	Low	≒21%	－ (γ)
J	BACKUPS LOST, STOLEN 事業者がバックアップファイルを毀損させたり，漏えいさせるリスク	Medium	≒24%	－ (γ)
K	UNAUTHORIZED ACCESS TO PREMISES 事業者の施設に簡単に侵入でき，機器にもアクセスできるリスク	Low	≒21%	－ (β)
L	THEFT OF COMPUTER EQUIPMENT 事業者の機器（サーバ，ストレージなど）が盗まれるリスク	Low	≒18%	－ (β)

K	UNAUTHORIZED ACCESS TO PREMISES 事業者の施設に簡単に侵入でき，機器にもアクセスできるリスク	Low	≒21%	－ (β)
L	THEFT OF COMPUTER EQUIPMENT 事業者の機器（サーバ，ストレージなど）が盗まれるリスク	Low	≒18%	－ (β)

リスク要因：ENISA のリスク分類のうち機密性に関するもの
ENISA 評価：ENISA のリスク分類における評価
利用者の不安意識：服部ら[9]による利用者の不安意識調査（4 択‥重大，中程度，軽微，ない）結果のうち，重大と回答した比率
クラウド化推定危険度：大学がクラウドを導入することにより機密性に関する危険度の推定増減指標

表 3 におけるクラウド化推定危険度欄で項番 G が±なのは，IT 係の堅牢さ（α）では事業者の方が勝ると考えられるものの，反対にそれがアッタクなどの攻撃の誘因になり得ると考えるためである．

表 3 でクラウド化により危険が高まると感じるのは A～C である．実際，これらは利用者の不安意識でも高い値を示している．しかし B については，正当な事業者であれば該当するとは考え難い．また C についても，α（IT 設備等の堅牢さ）の前提に立てば実際には大きなリスクにはなり得ないと考える．結局，A すなわち事業者の内部者によるセキュリティ違反が不安感の最大の要因と考えられる．

5.3 クラウド化に伴う情報セキュリティの不安解消に向けて

これまで述べてきたように，大学へのクラウド導入に際して懸念される最も大きな要因は，表 3 での危険度推定の前提 δ（担当者の顧客（大学）に対するロイヤリティ）に代表される人的要因に関するものである．これについて，クラウドサービスを提供する事業者に対して担当者への訓練充実や意識向上を求めることも重要ではあるが，基本的に異なる組織である以上，クライアントとしての介入には限界がある．そのため組織同士としては，結局，SLA（Service Level Agreement）の形で明示化することに帰結せざるを得ない．

SLA についてたとえば総務省の報告書[5]では，利用者の視点に立ち，SLA の在り方やセキュリティ・プライバシーの確保の在り方等として，QoS(Quality of Service)やセキュリティレベルに関するレイティング，データセンターの稼働率やパフォーマンス，データバックアップ・リストア，障害回復時間，障害通知時間等の標準化の必要性を主張している．しかしこのうちセキュリティに関する部分だけでも，大

学という組織特性を鑑みると一般的に標準化された SLA をそのまま適用できるとは考え難い．そのため大学としてクラウドを推進するためには，少なくてもセキュリティに関してだけでも SLA の整備に向けた情報共有と推進が求められる．具体的には，以下の項目の実施が必要である．

(1) いたずらな不安感を抑制するため，リスクの所在を明らかにしなければならない．そのためにはまず業務自体を分析し，業務における情報フロー，情報の性質，関与者等を明確にする．
(2) 情報フロー等に基づき，業務をクラウド化した際に想定される情報セキュリティリスクを明らかにする．
(3) リスク削減に有効な SLA を検討する．
(4) 通常の企業間同士と較べれば大学間の業務における多様性は低く，したがって情報セキュリティリスクも類似性が高いといと考えられる．そこで個別の大学が策定した SLA を，可能な範囲で大学間共有を図る．
(5) SLA はあくまで表現可能なことが対象であるのに対し，実際のリスク，特に不安感に関しては表現しきれない要素も多いと考えられる．そのため上記の取組みをしたとしても，不安が残る可能がある．そこで重要なのは，事業者やサービス形態，方式などに関する“評判（reputation)”である．これは曖昧な概念ではあるものの，日常の業務での実感を反映したものであり，客観情報にはなり得なくても参考情報としては極めて価値ある場合が多い．そこで前期の情報共有には，この評判情報も含める．

（1）～（3）は各大学が個別に推進できるが，(4)（5）は複数の大学が関係し，さらにはオープンな「場」が有効でもある．そのため場の構築も重要なポイントである．

6. おわりに

クラウド導入の大きな課題として，セキュリティ面も含めてしばしばリスクの増大が指摘される．もちろん従来と異なることをする場合，一般的には新たなリスク発生を考慮しなければならない．一方で，従来のままでいる，すなわちクラウド化しない場合のリスクも念頭に置くべきである．つまり費用などのコストも含めたトレードオフの関係を分析しなければならないが，そこで最も扱いにくいのが，主観に基づく要因である．その一例として本稿で取り上げたセキュリティ上の不安感があるが，その他にも従来からやり方の変更に伴う抵抗感などがある．

たとえばネットワーク管理者への聞き取りでは，学内で発生・消滅する情報をクラウド化によってわざわざ学外に流すことによるインターネット回線上のパケット増を招くことによる「呵責の念」を示されることがあった．確かに公共性の尊重という点からは尊重されるべき指摘ではあるが，インターネット上を流れる動画のストリーミング配信，P2P による大量のファイル交換，OS やアプリケーションソフトのダウンロードやアップデート情報などと比べると各個人による学外クラウド利用における通信量は少量であり，実質的には杞憂に過ぎないと考える．あるいは，クラウド化によって技術やノウハウの蓄積ができないというものもあった．確かにこの点は大いに憂慮すべき側面を持っているが，その一方で環境が変わる以上，個人として求められるスキルも変化しておりそれへの柔軟な対応が必要となっている．

いずれにせよ関係者の中にこのような感覚が事実として存在し，それがクラウド化の足枷になりかねないことは認識すべきである．そのためには今後，客観的データに立脚した分析だけでなく，このような主観的側面の強い課題にも積極的に対応すべきと考える．

参考文献

1) Mell, P. and Grance, T. : The NIST Definition of Cloud Computing, National Institute of Standards and Technology(2009).
2) 日経コンピュ-タ (706), 120-125, 2008-06-15
3) クラウドコンピューティング研究会:進化するクラウド情報基盤, 静岡学術出版(2011)
4) 経済産業省：「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」報告書,2010.8, http://www.meti.go.jp/press/20100816001/20100816001-3.pdf
5) 総務省：スマート・クラウド研究会報告書,2010.5, http://www.soumu.go.jp/main_content/000066036.pdf
6) ENISA：Cloud Computing: Benefits, risks and recommendations for information security, http://www.enisa.europa.eu/
（和訳 「クラウドコンピューティング：情報セキュリティに関わる利点，リスクおよび推奨事項」独立行政法人 情報処理推進機,2009.1）
http://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Computing%20Security%20Risk%20Assessment.pdf
7) ウィキペディア：「リスク」
http://ja.wikipedia.org/wiki/%E3%83%AA%E3%82%B9%E3%82%AF
8) 独立行政法人 情報処理推進機構：クラウド・コンピューティング社会の基盤に関する研究会報告書,2011.3,
http://www.ipa.go.jp/about/research/2009cloud/pdf/100924_cloud.pdf
9) 服部，原田：クラウドに関する情報セキュリティの課題の整理～アンケート調査結果からの分析～，情処学会研究会報告，Vol.2010-CSEC-51 No.6,2010/12/10