Executive Summary

本レポートは「クラウド時代の法制度と情報セキュリティ」に関して、㈱富士通総研から委託を受けた情報セキュリティ大学院大学が、学者や実務家をメンバーとする研究会を組織し、約 5 ヶ月にわたって集中的に討議した結果を取りまとめたものである。テーマのカバーする領域が広いため、本レポートで提起された問題点も幅広いが、経営者にとって必要な範囲で要約を試みる。

まず各章ごとに論点を整理すれば、以下の通りである。

・「総論」は、本レポート全体の導入部として、全体の鳥瞰図を与えるものである。まず、時としてバズワードになりかねない「クラウド」の概念を明確にし、クラウドの利便性が広く認識されている反面、セキュリティに関する不安が残っていることを、各種の調査結果から明らかにする。さらにユーザ企業から見たリスクの分類とガバナンスのあり方を考察し、クラウドのリスクが従来のものと基本的には異なるものではないが、その社会的影響は従来の比ではないことを指摘する。これはインターネットに内在する脆弱性とも関連し、基本的には「市場原理」をベースにした自律的仕組みで解決されるべきであるが、将来の姿として「ICT のユーティリティ（公益事業）化」に繋がる問題でもあることに、注意を喚起している。

・「各論 第 1 章 クラウド・サービス提供契約における法的諸問題」は、本レポートの中心テーマである「法的課題」を概観している。まずクラウド提供契約の特徴として、①約款の形態をとること、②オンライン契約であること、③SLA（Service Level Agreement）を内包すること、を指摘する。そして、以下の法的課題を摘出している。①約款の拘束力について、民法（債権法）改正の過程で、一定の条項について、その効力を制限することが提案されており、現在利用されているクラウド提供契約の条項についても、無効となるものがあり得るため注意が必要である。②オンライン契約における約款（利用規約）の扱いについて十分な議論がなされていないが、プロバイダは同意クリックを求めることで、リスクを低減できる。③SLA の性質について議論があるが、通常は契約の一部分と解すべきである。経済産業省の「SaaS 向け SLA ガイドライン」のチェックリストは、極めて有益である。

・「各論 第 2 章 クラウドコンピューティングの法規制とデータ所在地」は、法的課題のうちでも常に心配の種とされる「準拠法と裁判管轄」の問題を扱っている。まず、この両概念に関する諸学説を紹介し、必ずしも見解が一致するわけではないが、かといっ

て無原則と言えるほどでもないことを論証する。そして、どの説をとるにせよ結論がさほどかけ離れたものにはならない場合が多いこと、さらに契約によって問題を予め回避できる場合が多いことが指摘される。執筆者は、新たな現象＝新たな問題と捉えるのではなく、伝統的問題に包摂して扱うことができるか否かを考えることも必要だと強調している。これは、保守的であることに価値がある法学の分野で有益な示唆であるにとどまらず、クラウドに対する姿勢の一般論としても、有効と言えることかもしれない。

- 「各論 第 3 章 プライバシー・個人情報保護をめぐる諸問題」は、クラウドの登場と普及によって発生する法的課題のうち、プライバシーや個人情報保護に関する問題を扱っている。クラウドを提供する事業者（「クラウド事業者」）が、ユーザに関する個人情報を取得する場合や、クラウドを利用する事業者（「クラウド・サービス利用者」）がユーザの個人情報を取得し、当該事業者がそれらの個人情報をクラウド事業者において保存、管理する場合などが想定される。このような場合には、プライバシーや個人情報保護に関する様々な問題が発生することになる。しかし、こうした諸問題はクラウドに特有というよりも、電子商取引全体に共通の要素が多いものと考えられる。なお一部の論者は、クラウドへの個人情報保護法の適用を否定する説を唱えているが、これもまた極論と言うべきであろう。
- 「各論 第 4 章 クラウド・コンピューティングと著作権」は、前章と同様、法的諸問題のうち著作権に焦点を合わせたものである。電子的な取引が広まると、著作権侵害の主体が誰かが争点になりやすい。特にわが国では、いわゆる「カラオケ法理」によって、直接侵害行為を行なっているわけではないサービスの提供者が、責任を問われることがある。本章では、最近の最高裁判例である「まねき TV 事件」や「ロクラクⅡ事件」を踏まえて、クラウド事業者の責任のあり方について検討している。両判決は射程が狭く、クラウドには影響を与えないというのが執筆者の見解であるが、果たしてそのような解釈が一般的になるかは現時点では不明であるため、今後の注意を促している。
- 「各論 第 5 章 ユーティリティとしての諸問題」は、クラウドについて、しばしば電力や水道との対比がなされることから、そこに何らかの共通点があるのではないかという疑問からスタートする。そして、英語では utility、日本語では「公益事業」という概念が、何らかの形での「公的規制」を予感させることを指摘する。しかし、こうした規制を受け入れることは、クラウドがコンピュータ・サービスの一種である「自由市場」として、一度も公的規制を受けることなく発展してきた歴史からの、逸脱を意味している。果たして、そうした逸脱は望ましいことなのか、望ましくないとすればどのような対応策があるのか、を論じている。

・ 「各論 第 6 章 クラウド・ベンダーの差別化戦略」は、短いがユニークな章である。それは、「クラウド化したコンピュータ・サービスは、どのベンダーの提供するものでも同じになり、コモディティ化するのではないか。すると勢い先行者が優位に立つから、後発の日本のベンダーには勝ち目がないのではないか」という疑問に対する回答である。ここでは、わが国ベンダーのための活路として「付加価値の創造」を検討し、次の 5 つの方式を提案している。① crowd（大衆）の知恵の活用、②データ・マイニング、③知の構造化、④意味の抽出、⑤人間関係を中心にした関係性の追求。

以上が本論であるが、本レポートでは補論として、広い意味でクラウドに関連するテーマを併せて検討している。

・ 「補論 第 1 章 TDF からクラウドへ：名和小太郎氏ヒアリング結果」は、クラウドの法的諸問題を考える際に、先駆的論議として TDF (Trans-border Data Flow) の問題があったことを想起し、両者はどこが似ていて、どこが違うのかを検証しようとする試みである。本問題に詳しい名和小太郎氏を、自宅に訪ねて行なった質疑応答を取りまとめたものであるが、クラウドが昨日・今日の問題ではなく、その源流はかなり古いことが伺える。対談形式で読みやすく、堅い報告書の中で「息抜き」の効果もありそうである。
・ 「補論 第 2 章 サイバーセキュリティに関する ISP の責任」は、「法と経済学」の視点から ISP の責任論に関するサーベイ結果を紹介している。クラウドがインターネットを通じて提供される以上、サイバーセキュリティはクラウド事業者・ユーザの双方にとって重要である。政府と ISP の協力によるマルウェア除去が進み、日本は国際的にみてもボット感染率が低く、「サイバークリーンセンター（CCC)」の取組等が一定の成果を上げていたと推測できる。ボットネット感染率が他国よりも低いとなれば、国内にサーバを設置するクラウド事業者は競争上有利となる。しかし、CCC の活動は期限付きで、2010 年度で終了した。その活動を何らかの形で再開することが、日本のクラウド事業者にとっても重要であることを指摘する。
・ 「補論 第 3 章 EU におけるクラウド論議と日本への教訓」は、本レポート唯一の海外からの寄稿である。欧州委員会もクラウドの成長を、欧州産業成長の牽引役とみて推進しているが、欧州のデータ保護指令はプライバシー保護という社会政策的見地から、欧州内にある個人データの域外流出を原則として禁止している。欧州委員会は、産業界や第三国の Cloud Serive Provider（CSP、主にアメリカ）の要請に応え、2010 年に契約書に盛り込むべき標準条項を発表した。今後、CSP、そのサブコントラクター、クラウド利用企業とその顧客、などとの間の権利義務関係、欧州法の適用範囲など、実例を重

ねながら明確にしていくべき点は多い。日本の CSP が欧州に進出する場合、既にできた法に従うことは必要だが、今後生じる新たな事項に対しては、欧州との緊密な意見交換を通じ、相互に受け入れられる解決策を作り上げていく必要があることを指摘する。

こうした検討結果から、早急に結論を導くことは難しいし、早計でもあろう。しかし、少なくとも次のような教訓を指摘することは可能かと思われる。

- クラウドが騒がれる割には、法的課題は既に検討されていたものか、その延長上で解決可能なものが多いと思われる。
- しかし、騒がれるにはそれ相応の理由があると考えるべきだろう。その要点は、同じ問題であっても規模が違ったり、影響の拡散速度が違うことで、いわば「量が質に転化する」可能性が高いことである。
- その意味では、今回の検討は入り口に過ぎず、今後も事態の推移をみつつ検討を継続すべきである。

なお最後に一言だけ、付言したい。本レポートは、2011 年 2 月までは研究会の開催を主にし、3 月に入ってからは執筆者が担当部分を執筆することになった。その最後の段階で、3 月 11 日の大震災が発生した。この未曾有の事件は、クラウドについても多くの教訓を与えてくれるものと思われる。しかし、本レポートに生かすだけの時間的余裕がなかった。その点は、ご容赦をいただきたい。

目次

総論

情報セキュリティ大学院大学
田川義博

1.クラウドコンピューティングの分類と特徴

1.1 NIST（米国国立標準技術研究所：National Institute of Standards and Technology）によるクラウドコンピューティングの定義[1]

1.1.1 定義

クラウドコンピューティングについて統一されたものはないが、代表的な定義は以下の定義である。

・「クラウドコンピューティング」とは、（ユーザにとって）最小限の管理労力、あるいはサービス提供者とのやりとりで、迅速に利用開始あるいは利用解除できる構成変更可能な計算機要素（例えば、ネットワーク、サーバ、ストレージ、アプリケーション、サービス）からなる共有資源に対して簡便かつ要求に即応できる（オンデマンド）ネットワークアクセスを可能にするモデルである。」[2] また、この定義に続いて 5 つの特徴、3 つのサービスモデルおよび 4 つの展開モデルについて述べられている。

1.1.2 5 つの特徴(five essential characteristics)

・On-demand self-service

ユーザは事業者とのやりとりをしなくても自分だけで、サーバの利用時間やネットワーク・ストレージなどのコンピュータ能力を利用できる。

・Broad network access

利用はネットワーク経由で、携帯電話、ラップトップ PC や PDA のような異なる端末を通して行われる。

・Resource pooling

事業者のコンピュター資源は、マルチテナントモデルによって複数のユーザによって共有される。物理的および仮想的な資源は、ユーザの要求によりダイナミックに割り当てが行われる。ユーザは提供される資源の正確な場所についてコントロールできず、知ることもできない。しかし、より抽象化されたレベル（例えば、国、州やデータセンタ）では特定し得る。利用できる資源の例としては、ストレージ、処理、メモリー、ネット

ワークの帯域幅およびバーチャルマシーンがある。

・Rapid elasticity

コンピュータパワーは迅速かつ柔軟に、場合によっては自動的に、伸縮自在に提供される。ユーザにとっては、無制限にかついかなる時にでも利用できるように見える。

・Measured services

クラウドシステムでは、サービスの種類（例えば、ストレージ、処理、帯域幅）に応じた課金を行うことで、資源利用を自動的にコントロールおよび最適化している。資源利用は事業者とユーザの双方に透明性を確保することで、監視したり、コントロールしたり、報告したりすることができるようになっている。

1.1.3　3 つのサービスモデル

・Cloud Software as a Service(SaaS)

・Cloud Platform as a Service(PaaS)

・Cloud Infrastructure as a Service(IaaS)

注：SaaS、PaaS、IaaS の違いは一般的には以下のように区分されている。

図表 1：それぞれのモデルにおいてクラウド事業者・ユーザの提供区分

	SaaS	PaaS	IaaS
アプリケーション	事業者が提供	ユーザが提供	ユーザが提供
ミドルウエア、OS	事業者が提供	事業者が提供	ユーザが提供
インフラ（サーバー、ストレージ、ネットワーク）	事業者が提供	事業者が提供	事業者が提供

なお、SaaS 事業者が他のクラウド事業者のインフラを利用するケースも見られる。

1.1.4　4 つの展開モデル

・プライベートクラウド

クラウドのインフラはひとつの組織専用として運用されている。当該組織または第三者によって管理されており、オンプレミスの場合とそうでない場合がある。

・コミュニティクラウド

クラウドのインフラは、いくつかの組織によって共有されており、課題（例えば、ミッション、セキュリティ要件、ポリシーおよびコンプライアンス上の考慮）を共有する特定のコニュニティにサービスを提供する。当該組織または第三者によって管理されており、オンプレミスの場合とそうでない場合がある。

・パブリッククラウド

クラウドのインフラは、クラウドサービスを提供する組織によって所有されており、一般ユーザおよびひとつの大規模なグループが利用できる。

・ハイブリッドクラウド

クラウドのインフラは、二つ以上のクラウドの複合体（プライベート、コミュニティ、パブリック）である。インフラはそれぞれは独自のものであるが、データやアプリケーションのポータビリティを可能にするために標準技術または特許技術によって結合されている。

1.2 コンピュータの歴史におけるクラウドコンピューティングの位置づけ

経済産業省報告書においては、クラウドコンピューティングは、PC/Windows、商用internet/webに次ぐ、第３のICT変革であるとしている[3]。

また、小池良次氏は、コンピュータ利用の発展を、次のように整理している[4]。　①まずハード・ソフト一体であった時代から、②ハード・ソフトの分離が行われた。（ウインドウズはハードウエアの束縛から解放した。）この結果、メーカーが異なるコンピュータでもOSが同じなら、アプリケーションが相互に使えるようになった。しかし、OSが異なると互換性はなかった。③インターネットでは、OSの違いがあっても同じようにホームページが表示できるようになった。JAVAの仮想マシンを使えば、OSが異なっても一種類のソフトウエアを書くだけで済むようになった。これによって、ネットワーク依存型アプリケーションが多数出てくるようになった。④現在は、ソフトウエアがデータフォーマットやビジネスルールという束縛と戦っている段階。これを打破するのがXML。これらの束縛から逃れることができると、ソフトはコンピュータとインターネットが「ひとつの世界として動く」ため、必要に応じて複数のサーバに分けて処理できるようになる。この段階で、本格的なネットワークベースのソフトウエアの世界が広がる。これがパッケージソフトウエアの次にくるクラウドコンピューティングの時代であると位置づけている。

1.3 ユーザ企業から見たクラウドコンピューティング利用の優位点とされる事項[5]

① ユーザ企業として初期投資が抑えられる。また、資産計上が要らなくなるため、固定資産管理が不要になる。

② サービス導入のためのリードタイムが短いため、迅速なサービス開始が可能になる。

③ システム管理業務など運用要員を少なくできる。

④ 新商品のキャンペーンなど一時的な利用増に柔軟に対応できる。
⑤ 従量制料金なので、利用の多寡に応じたコスト負担になる。
⑥ 全体として、特にパブリッククラウドでは、クラウド事業者の規模の利益が大きいためコスト低減効果が生まれやすく、ユーザ企業の利用上のコスト負担が少なくなる。
注：クラウド事業者の方でも、安価なサーバーを自作してデータセンターを運用しているケースがあり、かつ、サーバの故障についてもその都度ではなく、定期的な整備を行うことで、人的なコストの低減を図るなど低コストの運用に努めている。

1.4 クラウドコンピューティングに適した業務領域[6]

クラウドコンピューティングに関しては、適した業務領域がある反面、現時点ではクラウド利用に十分な検討が必要な業務領域もあるとされている。例えば、機密データを扱うアプリケーション、高度なカスタマイズが必要なアプリケーション、複雑なプロセスやトランザクションが必要なアプリケーションがある。

また、一方で、社会的分野においては、クラウド化によって進展すると期待される業務領域として、複数医療機関でのカルテ共有、高度な画像診断、金融リスクの管理およびエネルギー管理がある。

注：この適用領域の考え方は、現状のクラウドを前提としたものであり、今後のさまざまな要素の変化によって変わるものと考えられる。

1.5 クラウドコンピューティングの利用動向

①現状のクラウドコンピューティング利用に関しては、ユーザ企業では基幹業務よりはフロント（情報系）システムの利用が多い。
②日米比較調査によれば、米国のクラウドサービス利用は日本の約 4 倍、また、利用内訳では、情報系システムでの利用は同程度にあるのに対して、基幹系システムでは、米国の方は約 2 倍程度高いとの結果になっている。

出所：総務省[2010]「スマートクラウド研究会報告書」p23

③ 情報セキュリティ大学院大学原田研究所が 2010 年 8 月に実施したアンケート調査結果として以下の事項が明らかにされている[7]。N＝316

・クラウド利用：すでに利用している（20%）、利用を予定している（6%）、未利用だが、利用を検討したい（41%）
・選定したいクラウド事業者：国内大手ベンダー（113）、自組織でプライベートクラウドを構築（49）、国内中小ベンダー（42）、Google（33）、通信キャリア（28）、

Salesforce.com(23)、自組織の情報サービス子会社(11)、海外大手ベンダー(9)、Amazon Web Services(6)、その他(17)

・クラウド事業者の選択で重視する上位項目:「障害が起きた時の対応が早い」、「月額費用が安い」、「技術力が高い」、「導入費用が安い」の 4 項目については、「非常に重視する」と「ある程度重視する」の合計が 90%を超えている。反面、選定に際して、「会社の知名度が高い」、「営業の提案力が高い」、「仮想技術を選択できる」に関して「非常に重視する」と「ある程度重視する」の合計は 50%を超える程度である。

・現在すでにクラウドコンピューティングを利用しているユーザの満足度については、事業者選択で重視する項目である「導入費用が安い」、「障害が起きた時の対応を早い」、「技術力が高い」に関しては、「非常に満足」と「ほぼ満足」の合計は、おおむね 60%前後である。ついで「月額料金が安い」の項目の合計は 50%超である。

・一方、「カスタマイズ等の実現スピードが速い」、「営業の提案力が高い」および「監査できる」に関しては、「非常に満足」と「ほほ満足」の合計で 30%ないし 30%を下回る水準となっており、「非常い不満」および「不満」とする合計も 20%弱を占めている。

・今後のサービス利用予定:SaaS(164)、PaaS(67)、IaaS(62)

1.6 実際のクラウドコンピューティング事例と提供事業者

＊PaaSのクラウド事業者としては、Google App Engine、Windows Azure Platformなどがあり、IaaSのクラウド事業者としては、Amazon Web Services、富士通オンデマンド仮想システムサービスなどがある。ただし、このPaaSとIaaSの境界は曖昧であり、例えばWindows Azure PlatformはIaaS寄りのPaaS、Amazon Web ServicesはPaaS寄りのIaaSである[8]。

＊実際にクラウド事業者として選定される可能性が高いのは、前述の情報セキュリティ大学院大学の調査では国内大手ベンダーであるが、刊行物やセミナーで紹介されるのは、上記の事業者であることが多く、ここに実際と喧伝される事業者とのギャップがあるように考えられる。

2. 本研究会において議論したテーマと項目

＊第 1 回:2010 年 11 月 19 日(金)

・研究会の趣旨、Asian Cloud Manifesto、Personal Data in the Cloud(富士通レポート)

・クラウドコンピューティングのセキュリティに関する法的諸問題の検討

＊第 2 回:2010 年 12 月 3 日(金)

・クラウド時代の情報セキュリティ・アンケート調査結果
・クラウドサービスの提供条件：公益事業との比較
・国境を超えるクラウドサービスの法的規制に関する準拠法と国際裁判管轄
＊第 3 回：2010 年 12 月 14 日（金）
・クラウドコンピューティング動向
・メンバーの問題意識の持ちより
＊第 4 回：2011 年 1 月 7 日（金）
・クラウドサービス提供契約における問題点
＊第 5 回：2011 年 1 月 21 日（金）
・総務省のスマートクラウド戦略とネットワーク中立性
＊第 6 回：2011 年 2 月 8 日（火）
・クラウドと著作権法
・クラウドと個人情報保護
＊第 7 回：2011 年 2 月 22 日
・報告書構成と分担に関する意見交換
・リスク・マトリックスに関する意見交換
・総論に盛り込むべき事項についての意見交換

3. クラウドサービスに関するユーザ企業が抱く不安とリスク

3.1 クラウドサービスに対する利用者の不安例[9]

＊システム運用に対する不安

クラウド事業者が運用管理を行うため、ユーザ企業はどのように運用がなされているのか知ることができないとの不安がある。

＊データの保存場所および保存方法に対する不安

クラウドサービスは、複数の利用者でシステムを共有する「マルチテナント方式」で運営されている。このため、各利用者のデータが確実に分離されているかが分からないとの不安がある。

＊インターネットを利用することに対する不安

インターネットは誰もが利用可能なため、利用者のデータが盗まれるとの不安の声がある。

＊サーバの差押えに伴うサービス停止に対する不安

2009 年 4 月、米国テキサス州において、FBI が CoreIP Networks 社のデータセンタか

ら機材等を押収したことにより、50 社の顧客に対するサービスが停止した。このように、外国の公権力によってサービスが突然停止するとの不安がある。

＊データの喪失に対する不安

携帯電話のデータが消滅する事例が発生している。このようなデータ消失がクラウドサービスで一般的に起こり得るとの不安がある。

＊アクセス不能およびデータ遅延に対する不安

クラウドサービスに障害が発生して、一時的にアクセス不能になるとの事件がいくつか起きている。このような障害が今後も発生するのではとの不安の声がある。

一般に想定されるアクセス不能およびデータ遅延の原因として考えらえるのは、以下のようなものが考えらえる。

・データセンタ所在地域の広域停電
・外国と日本の間の通信回線の遮断
・通信回線の帯域不足
・運用ミス
・予定外のサーバメンテナンス

＊稼働保証に対する不安

稼働保証が満たされなかった場合でも、実質的な利用料金の減額がなされるに過ぎない場合がほとんどである。稼働保証を下回ったことによりサービス利用者に損害が生じたとしても、実質的な料金減額が行われるだけではないかとの不安の声がある。

＊portability がないことによるサービスの利用継続に対する不安

標準化がなされていないために、他のクラウドサービスにアプリケーションを移すことが難しい。このため、クラウド事業者が倒産、買収または撤退した場合に、システムの利用を継続することができないのではとの不安の声がある。

＊portability がないことによるベンダーロックインに対する不安

これも標準化がなされていないために起因する不安である。

＊interoperability がないことによる相互協力の不存在に対する不安

これも標準化がなされていないために起因する不安である。

＊interoperability がないことによるマッシュアップに対する不安

これも標準化がなされていないために起因する不安である。

＊外国の公権力によるデータの取得、開示強制等に対する不安

クラウド利用者のデータがどこの国のデータセンタに保管されているか分からないため、外国の公権力による思わぬデータの取得、開示強制等が行われるという不安もある。

3.2 クラウドコンピューティングに関してユーザ企業がリスクと感ずる事項

前述の情報セキュリティ大学院大学のアンケート調査では、クラウドコンピューティングのセキュリティ上の脅威の大きさを他の形態と比較したが、次の結果となっている。

＊クラウドと自組織管理下にあるシステムとの比較では、クラウドの方が大きいとする回答が 36%、自組織システムの方が大きいとする回答が 23%、同じとする回答が 41%となっている。また、クラウドと従来のアウトソーシング（ホスティング）との比較では、クラウドの方が大きいとする回答が 27%、従来のアウトソーシングの方が大きいとする回答が 13%、同じとする回答が 60%となっていて、クラウドの方がセキュリティ上の脅威が大きいとする回答割合が多い。

図表 2　リスク評価について、「重大」とした割合の高い項目

＜組織的リスク＞ 第 1 位:事業者がサービスを中断したときの自組織のビジネスへのリスク 第 2 位：事業者の一方的な都合で、サービス内容が変更されるリスク 第 3 位:事業者が利用している他のクラウド事業者のトラブルの影響を受けて、サービス提供が中断したり、サービス内容が変更されるリスク 第 4 位:事業者にすべて任せてしまい、自組織で対応できなくなるリスク 第 5 位:事業者のコンプライアンス違反で、自組織も違反になるリスク 第 6 位：事業者に囲い込まれて、後日、事業者を変更できなくなるリスク
＜技術的リスク＞ 第 1 位：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 第 2 位：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 第 3 位：事業者への DDoS 攻撃でサービスが中断したり品質低下するリスク 第 4 位：事業者のリソース（サーバの CPU 能力やストレージ容量）が不足して、 その影響を受ける（処理速度が遅い、ファイルが保存できない）リスク

第 5 位：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
＜法的リスク＞ 第 1 位：事業者の違反や倒産などで、自組織のデータが差し押さえられるリスク 第 2 位：事業者と自組織の所在地（国）が異なり、裁判管轄や適用法令（例えば個人情報保護）が異なるリスク 注；この事項については、リスクがないとする割合も比較的高かった。これは前述したように、国内大手ないし中小ベンダーを選定する割合が高かったことの反映とも考えらえる。 第 3 位：事業者への法的な命令で証拠保全が必要となる（例えば法的機関へ自組織の情報が提出される）リスク 第 4 位：自組織への法的命令で証拠保全が必要となる場合、事業者側で証拠保全ができないリスク

＊また、クラウド事業者との SLA で重視するトップ 10 項目としては、①重大障害時の代替手段（197）、②サービス時間（178）、③平均復旧時間（154）、④サービス稼働率（140）、⑤サポート時間帯（129）、⑥バックアップの方法（108）、⑦ハックアップデータの保存期間（107）、⑧オンライン応答時間（106）、⑨ログの取得（96）、⑩障害通知プロセス（94）、

となっている。（N=316）

4. ENISA（欧州ネットワーク情報セキュリティ庁、European Network and Information Security Agency）のリスク分析

ENISAでは、「Cloud Computing：Benefits, risks and recommendations for information security」を 2009 年 11 月に公表した。この文書において、ENISAはクラウド化することで得られるセキュリティ上の 7 つの利点を挙げている[10]。

一方で、セキュリティ関連のリスク要因を「ポリシーと組織関連のリスク」、「技術関連のリスク」、「法的なリスク」および「クラウドに特化していないリスク」に分けて、37 項目挙げている。そして、この 37 個のリスク要因を発生確率とリスクが顕在化した場合の影響度の 2 軸で位置づけを行って、次のハイリスク 10 項目を抽出している[11]。

① ガバナンスの喪失

ユーザ企業はセキュリティ分野のコントロールについてもクラウド事業者に委ね

ることになる。

② ロックイン

現状では、他のクラウド事業者へ移ろうとしても、データ、アプリケーションおよびサービスのポータビリティを保証するツール、手順、標準データフォーマットもしくはサービスインターフェースは提供されていないために生ずる。

③ 隔離の失敗

マルチテナント方式によるリソースの共有はクラウドコンピューティングの特色であるが、ゲストホッピング攻撃などによってそれぞれのユーザのデータなどの隔離に失敗することが考えられる。

④ コンプライアンスに関するリスク

（業界標準や規制要件などの）認証を取得するための投資は、クラウド事業者が関連要件が適合的であるとの証拠を提示できなかったり、ユーザ企業に監査を認めないようなことなどがあれば、このリスクに晒される可能性がある。

⑤ 管理用インターフェースの悪用

パブリッククラウド事業者の顧客管理インターフェースは、インターネット経由でアクセス可能であり、リモートアクセスやウエブブラウザー関連の脆弱性と組み合わさった場合に、このリスクが増大する。

⑥ データ保護

ユーザ企業にとって、クラウド事業者によるデータの扱い方を効果的にチェックして、データが合法的に扱われていることを保証することが困難なことがある。この問題は、例えば連携しているクラウド間で、複合的なデータ転送を行う場合に深刻化する。

⑦ セキュリティが確保されていない、または不完全なデータ削除

ユーザ企業が要請しても、適切な、または、タイムリーなデータ削除が行えない場合がある。これは、対象データの複数のコピーがあったり、破壊すべきディスクに他の顧客データがある場合があるから。

⑧ 悪意ある内部関係者

発生する確率は低いが、内部関係者が悪意ある行為を行った場合には、重大な結果が生ずる可能性がある。

⑨ 司法権の違いから生ずるリスク（内容については修正）

個人情報保護のような法制度の違い、司法当局によるサーバの差押えによるサービス停止などのリスクがある。

⑩ ネットワークの途絶や混乱（内容については一部修正）

クラウド特有のリスクではないが、さまざまな原因によってネットワークが途絶したり、混雑したりすることで、ユーザ企業の事業継続にまで悪影響を及ぼすリスクがある。

5. ユーザ企業から見たリスク類型

クラウドコンピューティングの利用に関しては、 前 3 および前 4 においてさまざまなリスクがあることが分かった。このリスクを情報セキュリティで一般的な CIA 分類とクラウド事業者に自社の情報処理業務を依頼することに伴うリスクに分けて整理を試みる。

5.1 想定される機密性（confidentiality）・完全性（integrity）侵害と原因

・情報漏えい：マルチテナント方式の隔離の失敗、悪意ある内部者または外部からの攻撃や盗み見（不正アクセスなど）および管理用インターフェースの悪用のリスクがある。

例：Twitter 幹部が Gmail のパスワードを盗み、Twitter の機密情報が漏えいした。また、Gmail、Paypal、Apple/MobileMe、Amazon、AT&Tなどへのアクセスを通じて、クレジット番号、取引先のコンタクト、ミーティング報告書、転職/入社希望者の履歴書などを入手した[12]。

・データ消失：サーバのクラッシュ等に起因してデータが消失する場合がある。

例：ユーザ企業向けのクラウドではないが、MicroSoftのT-mobile向けのクラウドでユーザデータ消失およびデータバックアップサービスにおけるサーバ障害が原因で、連絡先、予定表、写真などの個人データが消失した[13]。

・データ削除：ユーザ企業が要請しても、適切な、または、タイムリーなデータ削除が行えない場合がある。

・クラウド事業者への法的命令で証拠保全が必要になり、法的機関へユーザ企業の情報が提出されたり、押収されたりするリスクがある。

・ユーザ企業への法的命令で証拠保全が必要になったが、クラウド事業者側で証拠保全ができず、法的命令に応ずることができないリスクがある。

・CAP定理[14]に基づく完全性に対する悪影響：クラウドコンピューティングは分散システムであることおよび可用性の二つが重視されるので、この定理が適用されるとすれば、完全性に悪い影響があると考えられるが、対抗策が全くないということではないように思われる。

5.2 想定される可用性(availability)侵害と原因

・ネットワークの途絶またはネットワークに起因するデータ遅延：クラウド事業者は、いずれのサービスモデルにおいてもネットワーク部分については自分も利用者の立場であって、クラウド事業者のコントロールが必ずしも及ばない。クラウドコンピューティングにおいてはネットワーク部分においてインターネットを多用するので、このネットワーク部分でのトラブルが発生すると可用性に大きな悪影響を及ぼす。

例：データセンタ所在地域の広域停電、外国と日本の間の通信回線の遮断、通信回線の帯域不足、運用ミス

・クラウド事業者のリソース不足（サーバの CPU 能力やストレージ容量）が不足することで、処理速度が遅くなったり、ファイルが保存できなくなるリスクがある。また、クラウド事業者の予定外のサーバメンテナンス等による可用性へ影響するリスクがある。

・事業者への DDoS 攻撃などのために、サービスが中断または品質低下のリスクがある。

・クラウド事業者の一方的な都合でサービス内容が変更されたり、クラウド事業者が他のクラウド事業者のサービスを利用している場合に、他のクラウド事業者のトラブルの影響を受けて、サービスが中断されたりするリスクがある。

・SLA によって保証されている稼働保証：どの程度の保証がなされているか、また、実際にこの稼働保証のレベルが実現できるのかの課題がある。また、稼働保証が守られない場合における補償レベルがどのようなものか、ユーザ企業に不利な内容になっていないかとの課題もある。

・ロックイン：現状では、他のクラウド事業者へ移ろうとしても、データ、アプリケーションおよびサービスのポータビリティを保証するツール、手順、標準データフォーマットもしくはサービスインターフェースは提供されていないために生ずるリスクがある。

5.3 クラウド事業者と利用することに伴うガバナンスやコンプライアンス・リスク

・クラウド事業者が運用管理を行うため、ユーザ企業はどのような運用が行われているのか必ずしも十分に把握・コントロールできないとのガバナンス上のリスクがある。

・（業界標準や規制要件などの）認証を取得するための投資は、クラウド事業者が関連要件の適合性に関する証拠を提示できなかったり、ユーザ企業に監査を認めないようなコンプライアンス上のリスクがある。

6. リスクガバナンス[15]

前 3 および 4 のリスクや不安に対して、前 5 においてユーザ企業の視点からのリスク類

型の整理を試みた。このリスク類型に対して、どのようなガバナンス手法によって対処したらよいかについて、6 において検討する。

6.1 ガバナンス[16]手法概念

注 15 のリスクガバナンス概念については、コーポレートガバナンスの視点からの概念である。これに対して社会全体におけるガバナンス手法については、市場機能（分権的意思決定）の活用、法・制度（集権的意思決定）の活用、企業などにおける自律的規律の活用の 3 手法がある[17]。 情報資産に関するリスクガバナンスに関しては、これに加えて、技術・標準の活用を加えた 4 手法の活用が期待される。

6.2 クラウドコンピューティングにおけるガバナンス手法の活用

市場機能の活用には、ユーザ企業のクラウド事業者選択、当事者間の SLA を含む契約内容のあり方およびクラウド事業者によるリスクガバナンスに関する自主的なガイドライン設定・標準化の推進がある。

また、ENISA 前掲報告書では、クラウドコンピューティングの契約の際に、注意を払うべき条項としては、セキュリティ違反の通知、データの転送、派生成果物（creation of derivative works)、管理者の変更(change of control)および法執行機関によるデータアクセスというような点に関する権利義務を挙げている。また、クラウドコンピューティングが利用できなくなった場合の法的責任の割り当て、または、インフラストラクチャに対する責任の割り当てにおいて、法的責任に関する標準的な制限が反映されているかも慎重に判断すべきとしている。

法・制度機能の活用には、法制度による履行強制および政府も関与する形でのリスクガバナンスに関するガイドラインの設定[18]、標準化の推進がある。

注：情報セキュリティに関する法律としては、「情報」を保護する個人情報保護法や企業の機密情報を保護する不正競争防止法があり、1987 年の刑法改正による追加規定、不正アクセス禁止法等がある。情報ネットワーク利用の規制法としては、特定電子メール送信適正化法や ISP 責任制限法、この他青少年を保護する法制度、さらには、通信の秘密を規定する電気通信事業法や電波法がある。また、内部統制に関する法律として、会社法や金融商品取引法がある。なお、クラウドコンピューティングに特化した法律は現時点ではない。

前述のようにリスクガバナンスの設定・標準化に関しては、市場機能の活用による場合と法・制度機能の活用による場合の両方があるが、実際には日本では政府が何らかの形で関与するガイドラインが多い。また、企業の自律的規律については、コーポレートガバナ

ンスや会社法などにおける内部統制と関連する。クラウドコンピューティングに関しては、クラウド事業者とユーザ企業の双方の自律的規律維持が課題になる。

6.3 ガバナンス手法の相互関係

前述したように、クラウドコンピューティングに特化した法は現時点ない。ENISA前掲報告書は、「クラウドコンピューティングに関連する法的な問題点の多くは、目下のところ、契約内容の評価（すなわち、複数のプロバイダーが提供するサービスの比較時）または交渉により解消されている。」[19]と述べている。また、この指摘は、市場機能と法・制度機能とは相互に補完関係にあることも意味している。

この現状をふまえ、ユーザ企業は、当面市場機能の活用を図ることが重要である。すなわち、導入検討時および契約締結時においては、クラウド事象者の選定や契約条項とその内容について不測の損害を避けるために、十分な検討をする必要がある。

また、利用時においては、契約条項をベースに、クラウド事業者からの開示情報やユーザ企業自体がモニタリングを行い、前述したリスクが顕在化しないような運用に留意する必要がある。

なお、クラウド事業者のパフォーマンスがユーザ企業の期待を大きく下回る場合に、ユーザ企業はクラウド事業者の債務不履行ないし不完全履行を理由として、契約を終了する選択肢もあり得る。しかしながら、前述したように、現時点では標準化が進んでいないためロックインされて、スムーズに他のクラウド事業者と契約したり、自社システムに戻したりする場合に大きな支障が出ることも考えられる。このため、契約時に信頼できるクラウド事業者を選定する必要性はそれだけ大きいと言える。

ユーザ企業及びクラウド事業者の自律的な規律維持[20]は、監査機能の充実を含め、両者のwin-winの信頼関係を構築するうえではきわめて重要である。 他のガバナンス手法の充実とあいまって、クラウドコンピューティング市場の発展につながることが期待できる。

さらに、ロックイン問題を解決などには、今後の技術・標準化の進展によって解決に向かうことが期待される。

6.4 法・制度機能の活用

ENISA前掲報告書では、リスクを組織的リスク、技術的リスクおよび法的リスクの 3 区分でリスク要因を整理している。この法的なリスクとしては、「証拠提出命令と電子的証拠開示」、「司法権の違いから来るリスク」、「データ保護に関するリスク」および「ライセンスに関するリスク」の 4 項目を挙げている。また、その付属文書において、5 つの法的な課題を挙げている。すなわち、①データ保護（可用性と完全性、最低水準

または保証）、②機密性、③知的財産権、④クラウド事業者の過失（ユーザ企業が自社の顧客に対する責任問題が発生）、⑤クラウド事業者の他へのアウトソーシング[21]。併せて、前5における不正アクセスによる情報漏えい、法的命令に基づく証拠保全、外部者のDDoS攻撃などは、直接に法・制度によって対処するリスクである。このような法的リスクの考え方はいわば狭義の法的リスクというべきものである。

これに加えて、例えば、先述のように契約条項の整備というような市場機能の活用によりガバナンスを行おうとしても、契約条項の履行が行われない場合があり得る。ユーザ企業は、損害を避けるために、履行請求なり、債務不履行・不完全履行を理由として、裁判所に訴訟提起をするなどの法的紛争解決の手段に移行するケースも生ずる。このように当事者で紛争が生じた場合で、市場機能が十分に働かない場合には、市場機能の補完的機能として、法・制度機能の活用が必要になる場合がある。

クラウド事業者とユーザ企業の双方の自律的規律維持についても、同様に、法・制度機能は補完的機能を有する。これが、クラウドコンピューティングにおける広義の法的問題である。したがって、この広義の法的問題を含めて、法・制度機能の在り方を検討することが望まれる（クラウド事業者とユーザ企業の間で結ばれるサービス提供契約をめぐる諸問題については、各論1を参照）。

以上の観点を踏まえたうえで、民事、刑事、行政の3つの法的分野の視点から、前6で整理したリスク類型の各項目について、個別に検討することが必要である。

7. クラウドのリスクと従来のコンピュータネットワークシステムのリスクの比較

7.1 オンプレミス・システムや従来のアウトサーシング（ホスティング）との比較

前述の情報セキュリティ大学院大学によるアンケート調査では、クラウドコンピューティングを利用した場合に、セキュリティ上の脅威が多いと考えるユーザ企業が多かった。

前1ではクラウドコンピューティングの利点、前3～6ではクラウドコンピューティングに係るリスク類型やそれに対するガバナンス手法の問題について考察した。

従来システムとリスクの大きさの比較を行う場合には、クラウドコンピューティングのリスク類型において、それぞれのガバナンス手法がどの程度有効なのかによって、結果が左右される。

クラウドコンピューティングに関するリスクやセキュリティについては、国際的なセキュリティ関連の事業者団体であるISACAの報告書では、別に新しい問題ではなく今日の企業システムにおいても存在する問題である、と述べている[22]。

前5におけるリスク類型を見ると、従来システムとの比較で、リスクが大きくなってい

るとは必ずしも言えないように思われる。すなわち、クラウド事業者がどの程度ユーザ企業の期待に応えるための取り組みを行うことに依存しているのではないかと思われる。この意味では、クラウドコンピューティング市場の発展は、クラウド事業者の自律的な規律維持が極めて大きな役割を果たすのではないだろうか。

7.2 クラウドコンピューティングにおけるリスクガバナンスの特徴

企業をはじめとして、経済社会活動全体においても、コンピュータ・ネットワーク（ICT）をより多用しており、それだけにこの可用性に支障が生じた場合の悪影響は大きなものがある。

今後、クラウドコンピューティング市場が拡大して、多くの企業などが利用することになれば、クラウドコンピューティングの情報セキュリティが損なわれた場合には、ユーザ企業に同時多発的に被害が及ぶ。このため、可用性が損なわれた場合などは、各ユーザ企業の事業継続性や経済社会活動全般に対する悪影響が広範に広がるため、個々の企業だけではなく、経済社会全体のリスクが大きくなる。このため、クラウドコンピューティングの情報セキュリティの重要性は従来よりも格段に大きくなる。(この情報セキュリティに関する ISP の責任問題については補論 2 参照)

したがって、対策としても、リスク顕在化防止という予防的な対処策に加え、リスクが顕在化した場合の障害耐性（resilience）をどう高めるかが、重要課題となる。

8. クラウドサービスの将来

8.1 クラウドコンピューティングが経済社会へ与えるインパクト

経済産業省のある研究会[23]では、「クラウドコンピューティングが実現する新サービスと新しい社会像」として、①万人がイノベーションに参画する社会」、「個人生活の便利さ、豊かさと社会全体の効率化が両立する社会」、「人と人とがつながり、全ての市民が社会参加する社会」の三つを挙げている[24]。

また、このクラウドコンピューティングが普及すると、ユーザ企業に対しては、競争環境と産業構造の変化を促し、既存のIT業界の構造転換が求められるとされる。[25]

8.2 クラウドコンピューティング普及の視点からの課題

1(3)(4)で述べたように、現時点では、クラウドコンピューティング利用は、まずは情報系システムから導入が始まり、今後、基幹系システムへの利用も進む方向にある。また、クラウドコンピューティングを利用することで、社会的分野の情報化が進むことが期待さ

れている。しかしながら、現時点では、機密データを扱うアプリケーションをはじめとして、クラウド化に慎重に対処すべき業務領域もあるとされている。

さらに、ユーザ企業においては、SaaS、PaaS、IaaSおよび自社システムが混在している。このなかからいずれを選択するかは、サービス品質、コスト、セキュリティ、事業継続性および法・制度的などの要素など考慮して行われている。今後はこれらの判断要素における変化によって、選択にも変化が生ずるものと考えらえる。したがって、クラウドコンピューティングの普及を図るためには、それぞれの判断要素におけるクラウド化への阻害要因を解消または軽減していくことが必要である。そのためには、いくつかの課題を解決する必要がある。

8.3 標準化問題

その一つの課題が標準化の問題である[26]。　現在、標準化については、Cloud Security Alliance(CSA)など多くの国際団体によって検討が進められている。標準化が進むと相互運用性が強化されて、ロックインの解消などが期待できる。しかしながら、総務省のスマートクラウド研究会報告書では、クラウド技術の標準化は、クラウド事業者によるロックインなどは排除できるものの、過度の標準化・共通化は、サービス革新や技術革新を阻み、クラウドコンピューティングの多様性が損なわれる恐れがあり、オープン標準で不足する機能は、クラウド事業者が付加価値サービスとして提供する「協調と競争」を旨とする市場環境の実現が必要と述べている[27]。　（この指摘は、各論6「クラウドの差異化戦略」に関連する論点である。）また、同報告書では標準化の検討項目として、SLAの在り方、セキュリティ・プライバシーの確保および相互運用性の確保の三つを挙げている。

標準化が進めば、クラウド間連携がより容易になり、クラウドコンピューティングの高度化も進むものと思われる[28]。

8.4　インターネットの脆弱性

自社の情報システムでも、クラウドコンピューティングでも、通信部分はインターネットを利用するようになっている。クラウド事業者でもあるGoogleは、グローバル・クロッシング社から大量の国際回線を購入したり、2008年にはKDDIなどと日米海底ケーブルの建設プロジェクトに参加したり、また米国内の光ファイバーケーブルを大量に取得して、通信回線部分にも一部進出していると言われている[29]。　しかしながら、Googleでもクラウド事業者として、自社保有ネットワークですべてのネットワークをカバーすることはできない。

クラウド事業者にとっては、ユーザ企業に対しては、ネットワーク部分を含めてサービスを提供しているが、この部分についてはアウトソースせざるを得ない。このため、クラウド事業者にとっても、このネットワーク部分については直接的にはコントロールすることができない。

このクラウド事業者の直接のコントロールが及ばないインターネットに関しては、P2P通信や画像利用などによってトラフィックが急増しており、設備容量の増強が迫られているが、その費用負担[30]を巡って、いわゆるネットワーク中立性の議論がなされている[31]。

また、インターネットは従来からいつかはクラッシュすると言われながらも、クラッシュせず利用されてきた。しかしながら、サイバーテロのなかでもネットワークの脆弱性を狙った攻撃がより大規模に行われる可能性は依然して消えていない。このようなインターネットの設備容量と脆弱性の問題に注目していく必要があると考えられる。

8.5 インターネット・トラフィックの変化

Chris AndersonとMichael Wolffは、インターネット・トラヒックの内容が、ウエブ利用から特定アプリへシフトし、このアプリの多くはクローズドで、しばしば独占的である、と述べている。また、5年のうちに、モバイル機器からのアクセスがPCからのアクセス数を上回るとの予測も紹介している[32]。

今後のユーザ端末がPC中心からモバイルシフトするとの予測されているため、垂直統合的なビジネスモデルがクラウドコンピューティングでも広がる可能性がある。

また、情報通信産業では、従来のモジュール化の流れが一転して、統合に回帰する動きがあり、クラウドコンピューティングもこの統合化の例であるとの指摘もある[33]。

8.6 各国法制度の違いおよび紛争解決の裁判管轄並びに適用法令

クラウドコンピューティングは、国境を超えることが通常であるため、各国の法制度の違いによって、日本では合法的な行為が、他国では違法となる場合があり得る。特に、注意すべきとされているのは、個人情報保護に関するEU指令、米国のPatriot法、外国為替および外国貿易法などがある[34]。　逆に、諸外国では実施例があるものの、日本では著作権法ではなお違法の可能性があるとされる例もある。（個人情報保護に関しては各論3、著作権に関しては各論4、EUのデータ保護指令における域外適用問題については補論3参照）

また、政府のクラウドコンピューティング利用において機密情報やセンシティブな個人情報が扱われる場合には、データを保管するのは、国内のサーバに限定するべきとの考え

方もある。

さらに、紛争が生じた場合には、裁判管轄とどの国の法令が適用されるのかについても分かりにくさもある。(この準拠法と裁判管轄をめぐる諸問題については各論 2 参照)

8.7 クラウドコンピューティングのユーティティ化問題

(この問題は、各論 5 で詳細に論じられている)

クラウドコンピューティングの発展を、電力がユーティリティ化の歴史と比較して論じているのが、ニコラス・カーである[35]。

カーは、まず、電力でも初期は技術規格、広範なネットワーク、一元的供給技術のいずれも欠いていたが、一元化することで得られる規模の利益が巨大であるため、かなり長い時間がかかったが、次第に現在のような長大なネットワーク網によって電力供給が行われるようになったとしている。そして、電力と IT は両者とも汎用技術(general purpose technology)であるが、電力とクラウドコンピューティングは、ネットワーク経由で遠方からでも効率的に電力なりサービスを供給できること、コントロールが集中化することが共通している。

しかしながら、電力とクラウドコンピューティングには相違点もある。それは、電力はエネルギーを供給するだけで、その電力がどう使われているかには関わらない。このことは、今回の東北関東大震災での計画停電の混乱を見るとよく理解できる。

一方、クラウドコンピューティングは、ネットワークというよりも、むしろコンピューティングの方に付加価値が存在しているため、クラウド事業者はここにビジネス的な重点を置いていることが電力と異なる点である。

また、カーは、コンピューティングがますますユーティリティになるにつれて、コンピューティング資産の多くは、世界中に点在し外国の管轄下に置かれるようになる。このことは、国家の安全と主権に対して新たな難題を提起するとして、国に経済を動かしているコンピュータやソフトウエアを自国で直接管理することを止めてしまって平気なのかとの問題提起を行っている[36]。

報告書の構成

本報告書は、2010 年 11 月から 2 月にかけて 7 回開催された研究会における討議を基礎にして、研究会の構成員が分担して報告書の作成を行った。まず、本総論に続いて、各論を 6 篇を、次いで、補論として 3 篇の論文を収録している。さらに、付属資料として、議事録等を収録した。

[1] The NIST Definition of Cloud Computing[2009]
http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf
[2] 日本語訳は、IPA[2010]「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」による。
[3] 出所：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]p16
[4] 出所： 小池良次[2009]『クラウド：グーグルの次世代戦略を読み解く、2015 年の IT 産業地図』
[5] 出所：各種資料により作成
[6] 出所：講演での IBM 社の指摘
[7] 「情報セキュリティ調査の実施について」 http://lab.iisec.ac.jp/~harada_lab/survey.html
[8] 出所：中田敦「自前のアプリも動く PaaS 型 IaaS 型躍進」、ITPro
[9] 出所：寺本振透編集代表/西村あさひ法律事務所著[2011]『クラウド時代の法律実務』p25～32
[10] ①大規模化（規模が大きいほどより低いコストで実装できる。）、②市場での差別化要因となるセキュリティ（機密性、完全性、障害耐性（resilience））、③標準化されたオープンインターフェースが提供できる、④セキュリティ対策のためにリソースを動的に再配分できる、⑤証拠収集が効果的にできる、⑥最新のパッチ設定などの最新のセキュリティ設定ができる、⑦リソースの集約化はデメリットもあるが、様々なセキュリティ・プロセスを容易にかつ低コストで適用できる。
[11] ENISA 報告書でハイリスクとされる項目は、マトリックスによる評価で 8 項目、個別評価で 9 項目および Executive Summary で 8 項目が挙げられている。しかしながら、3 つの評価ごとに取り上げられている項目はそれぞれ異なっており、統一が取れていない。
本総論では 3 つの評価で 2 つ以上ハイリスクとされた 10 項目を取り上げている。
[12] 出所：百瀬孝三[2010]「クラウド・セキュリティ概要」
[13] 出所：百瀬孝三　前掲資料
[14] CAP 定理とは、データの一貫性、システムの可用性、システムを分散することの三つの要素のうち、一時点では二つの要素しか実現できないとする定理である。
[15] 本報告書では、リスクガバナンスという用語を用いるが、検討対象は「情報セキュリティ」分野である。企業経営における「リスク」と「情報セキュリティ」の位置づけおよびガバナンスの意味については、以下の通りとされている。

企業経営の主目標は、（中略）「企業価値の向上」及び「社会的責任の遂行」にあり、これを支える重要な取組の一つにリスク管理が位置づけられる。
様々なリスクの内、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み＊を構築・運用することを情報セキュリティガバナンスと位置付ける。（＊経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを指す）
出所：経済産業省情報セキュリティ政策室編[2009]『情報セキュリティガバナンス』p236

この定義では、情報セキュリティは情報資産に係るリスクを管理するものであること、また、ガバナンスというのは経営者による方針決定、組織内モニタリングの仕組みおよび利害関係者に対する情報開示と利害関係者による評価を意味している。

[16] ガバナンス概念については、多義的ではあるが、「政府と民間組織との新しい関係を指す。同時に統治にかかわる多様な構造や原理をまとめあげていく能動的な働きかけ、それらの新しい連携を調整し統御する技法（後略）」とされる。出所：山口二郎/宮本太郎／坪郷實編著[2005]『ポスト福祉国家とソーシャル・ガヴァナンス』p2
[17] この市場機能など 3 機能の活用の概念については、以下の文書を参照。RISTEX(社会技術開発センター)「企業における情報セキュリティの実効性のあるガバナンス制度のあり方」（研究代表者林紘一郎） p4。
[18] 例えば、「ASP・SaaS の安全・信頼性に係る情報開示指針」[2007]（総務省・業界団体が合同で設立した ASP・SaaS 普及促進協議会）、「SaaS 向け SLA ガイドライン」[2008]（経済産業省）、「ASP・SaaS における情報セキュリティ対策ガイドライン」[2008](総務省)、「データセンターの安全・信頼性に係る情報開示指針（第 1 版）」[2009]（総務省）、「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」[2009]（総務省）、「クラウドサービス利用のための情報セキュリテ

ィガイドライン（案）」[2010]（経済産業省）など、クラウドコンピューティングの立ち上がりに向けて、いくつものガイドラインが公表されている。

[19] 日本語訳は、IPA 前掲書による。

[20] ユーザ企業の工夫としては、アプリケーション・レベルの監視の仕組みをオープンソースの監視ツールを利用して自作したり、セキュリティがブラックボックス化しやすいので、100%安心できないため、データの暗号化を行ったりしている例が、各種セミナーなどで紹介されている。

[21] ENISA 前掲報告書　ANNEX1- Cloud computing- Key legal issues 参照。

[22] 出所：ISACA[2009] “Cloud computing: Business Benefits With Security, Governance and Assurance Perspectives” p7

[23] 経済産業省前掲報告書第 2 章

[24] この新しい社会像を描くうえでのクラウドコンピューティングの具体例は、いずれも医療、交通、農業などの応用例が挙げられている。これは、1（3）のクラウドコンピューティングに適した分野として、社会的分野を挙げていることと符合している。

[25] 注 3 報告書 p24～26 参照

[26] 標準化動向については、前掲経済産業省報告書 p41～43 参照

[27] 出所：総務省[2010]『スマートクラウド研究会報告書』第 5 章

[28] このクラウド間連携を、クラウドインテグレーションと呼んで、今後 3 年後ぐらいに市場が立ち上がるとの見解もある。出所：佐藤秀哉「クラウドブームはあと 3 年、その先に二つの方向」日経コンピュータ 2010 年 9 月 15 日号 p50

[29] 出所：小池良次前掲書 p106～109

[30] 総務省[2008]「インフラ設備に必要な設備投資コストの負担問題」ネットワークの中立性懇談会資料

[31] 谷脇康彦[2009]「ブロードバンド市場におけるネットワークの中立性と競争政策」、慶応義塾大学メディアコミュニケーション研究所紀要参照。

[32] 出所：Anderson, Chris and Michael Wolff “The Web is Dead. Long Live the Internet.” Wired Sep.2010

[33] 田中辰雄[2009]『モジュール化の終焉：統合への回帰』参照。なお、本書は富士通総研との共同研究の成果物である。

[34] 出所：注 3 経済産業省前掲報告書 p27～34。この他にも、米国では、電子通信プライバシー保護法、連邦情報セキュリティ管理法、連邦民事訴訟規則、米国公認会計士協会基準第 70 号（SAS70）など多数ある。出所：下道高志「クラウド時代の企業 IT ガバナンス」、ITPro web 情報

[35] Carr , Nicholas[2008] “The Big Switch: Rewiring the World from Edison to Google”、村上彩訳、ニコラス・カー[2008]『クラウド化する世界：ビジネスモデルの大転換』

[36] 1980 年代においてコンピューティング利用についての国家の安全や主権の観点から、OECD を中心にして論じられてのが、TDF(Trans-border Data Flow)の問題である。補論 1 の「TDF からクラウドへ」参照。