論稿

クラウド統制と監査について

日本マネジメント総合研究所　理事長
戸村　智憲

はじめに

日本においても、定額給付金のシステムやエコポイントの付与システムなどの地方自治体や中央官庁などで採用・活用が進み、大手ＩＴ企業がこぞって大々的に参入・展開を進めるクラウドコンピューティング（以下、クラウドと略す）。

テレビＣＭや新聞記事・広告で毎日のようにクラウドについて扱ったものを目にするが、なかなかクラウド自体の理解は進んでいないのが現状である。

経営の現場では従来のＩＴのように初期費用を多額に投じて買って備えて使うことなくとも、初期費用０円（クラウドによって異なる）で「賢く安く借りて使う」クラウドに続々と手を伸ばしている。

その一方、内部監査人や外部の監査人（監査法人など）では、いっこうにクラウド自体の理解が進まず、現場で用いられているクラウドをどう監査すべきかについて考えが及ばない方々も多く見られる。

そこで、本稿では、クラウドそのものについての解説とともに、ＩＴ統制から一歩進んだクラウド統制の在り方や、クラウドにおける監査対応についても解説する。

〔1〕クラウドコンピューティングとは何か？

まず、クラウドの定義についてであるが、米国のＮＩＳＴやガートナー社の定義をはじめ、各ＩＴ企業や団体が様々な定義を打ち出しており、唯一絶対たる業界標準的な定義がないといっても良いのが現状である。

うがった見方をすれば、各ＩＴ企業や団体にとって、自らに都合の良い解釈で営業・事業展開がしやすいよう、クラウドが定義されていることもある。

加えて、クラウド提供側のＩＴ技術に偏った定義の仕方もあれば、クラウド利用側（クラウドユーザー側）から見たクラウドの定義もある状態である。

また、一言でクラウドといっても、インターネットを介して第三者・業務委託先のＩＴ資産を活用する「パブリック・クラウド」もあれば、自社内のＩＴ資産を効率的・効果的に活用するために、昔流にいえばＩＴ資産のシェアード・サービス化をする「プライベート・クラウド」もある。

本稿では、クラウドと称した際、基本的には前者を指すものとして、クラウド提供側というより、読者諸氏の視点、つまり、クラウドユーザー側の視点から解説を進めていこうと思う。

1．クラウドの定義

さて、ここでクラウドユーザーの視点から、本稿におけるクラウドの定義についてまとめておく。総務省から業務委託を受けてクラウドの普及啓発に努めているＡＳＰＩＣの例を基に、クラウドは次のような定義づけとなる。

【クラウドの定義】

クラウドとは、ＡＳＰやＳａａＳやユーティリティ・コンピューティングなど、データセンターのハードウェア・ソフトウェアの集合体のこと

※ＡＳＰ：Application Service Provider

※ＳａａＳ：Software as a Service

このような定義は定義として、要するに、少し噛み砕いていえば、①自社でサーバーやお金のかかるＩＴ機器・ＩＴソフトなどを持たず、②インターネットの向こう側にあるＩＴサービスを賢く安く借りて使って、③拡張性も縮小性（使えなければやめればいい）も備えたＩＴのこと、というようなものがクラウドである。

また、クラウドにおいては、基本的には使用する人数や分量（ＩＤ数など）の分だけお金を払えばよく、バージョンアップもメンテナンス（ＩＴ統制でいう運用・保守）もすべて固定月額内でクラウド提供側が対応してくれるもの、ということもクラウドの特徴である。

何となくまだピンと来ない方のために、かなり平たくクラウドをたとえると、クラウドは企業で用いられる営業車にたとえることもできよう。

これまで多額の初期費用を投じて購入していた営業車を、カーリースとして月額使用料だけで手配できるようにしたもの、というのが、語弊を恐れず「賢く安く借りて使う」クラウドのたとえである。

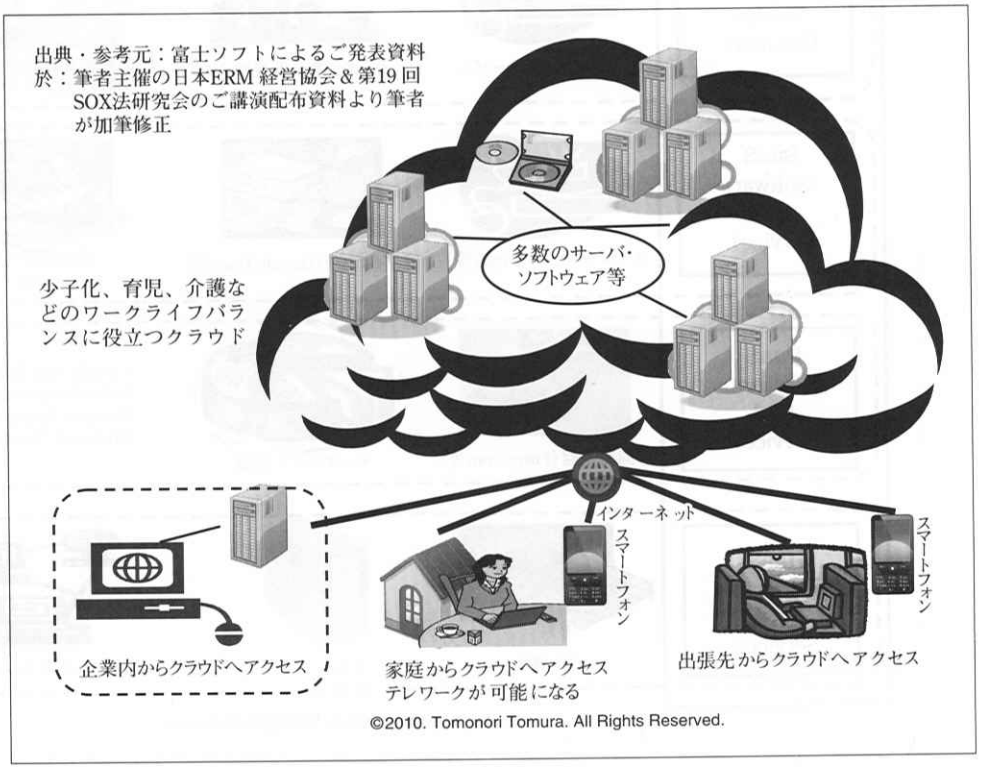
つまり、月額固定費用内で、営業車の整備・修繕（メンテナンス）がカーリースの提供企業側の負担で行ってくれるというような形態がＩＴにおけるクラウドのようなものである。

大まかなクラウドの概念図は図１にまとめておいたのでご参照いただきたい。

2．クラウドの類型

さて、クラウドについては、担当部署ごとに異なるクラウドの類型を指しており、監査の際にどの部署がどんなクラウドについて述べているのか混乱しがちなケースが散見される。

＜図１＞クラウドの類型例



そこで、クラウドの類型例をここで提示しておく。もちろん、呼称や分類形式は様々に成される可能性があるが、本稿における分類として図２にまとめておく。

図２におけるＡＳＰとＳａａＳは、いってみれば、インターネットを介してＩＴソフトをリースで借りて使うようなものである。また、ＰａａＳとＨａａＳ（又はＩａａＳ：Infrastructure as a Service）は、インターネットを介してＩＴの開発基盤やＩＴ機器をリースで借りて使うようなものである。

大くくりにまとめていえば、営業部や経理部などの現場では、クラウドといえばＡＳＰやＳａａＳを指し、ＩＴ部門ではＰａａＳやＨａａＳを指している、といっても良いであろう。

監査人としては、各現場のクラウドに関する監査をする際に、どの類型のクラウドを指しているかを意識しておくと良い。

３．国策として進められるクラウド

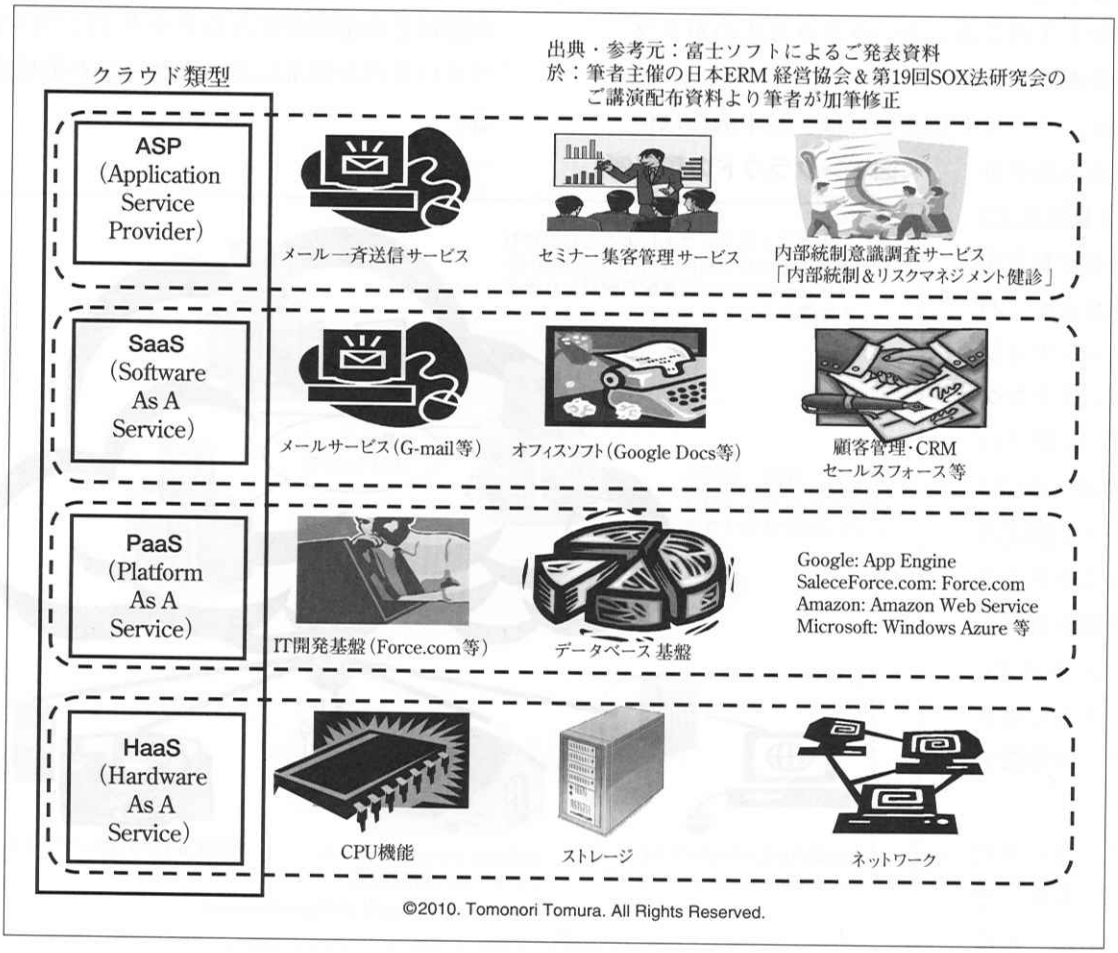
既に読者諸氏においてはご存じの方も多いであろうが、クラウドは単なるはやり言葉（バズ・ワード）ではなく、日本において国策として進められているものである。

一例としては、経済産業省（以下、経産省）において、クラウドを活用することで国際競争力や経営体質の強化を図るため、「Ｊ－ＳａａＳ」を展開している。

これは、日本発のクラウドを普及啓発しようとするもので、簡単な勤怠管理システムから本格的な基幹システムまで様々ある。

また、総務省でもクラウドに関する研究会が活動を深めており、経産省では医療・教育・行政・防犯など多様な面でクラウド活用の推進を提言し、予算が厳しい組織において、

＜図２＞クラウドの類型例



ＩＴ化を進めて経営・運営の高度化を図る施策が提示されている。

その他、霞が関クラウドや自治体クラウドなど、中央官庁や地方自治体でもクラウド活用が本格化してきている。

そのカギは、クラウドが圧倒的に安く開発期間も短く、開発の成功率も高いため、予算が限られていても高度なＩＴ活用を行いやすいことにある。

筆者としては、予算の厳しい時代にあって、リストラすべきは頭脳流出に直結する人材ではなく、従来型の多額の資金を必要とするＩＴ資産であり、クラウドを安く借りて財務的にも安定して活用することが効率的・効果的な経営の一手になると考えている。

その方が、日本版ＣＯＳＯモデルでいう「業務活動の有効性・効率性」の内部統制の観点からも、また、「資産の保全」の観点からも、企業経営においてより望ましいことである。

〔2〕高負荷なＩＴ統制からクラウド統制へ

ここまで、クラウドについての初歩的内容についてふれてきたが、少し話を進めて、筆者が世界初で提唱した「クラウド統制」（®戸村智憲）について解説しておこう。

ここで、まず、筆者がなぜ従来型のＩＴ統制対応ではなく、クラウド統制を進めるべきと考えるに至ったかについての背景を述べておこうと思う。

1．Ｊ－ＳＯＸ監査指摘での既存ＩＴ統制の課題

筆者はＪ－ＳＯＸが人口に膾炙する以前より、内部統制について監査法人の代表社員をはじめ、東京を中心に九州から北海道に至るまで、全国各社の監査部門やＩＴ部門などの内部統制指導や監査法人からの監査指摘の対応指導などに当たってきた。

現場から見えてくる問題と、Ｊ－ＳＯＸ監査本番以降に監査法人が指摘してきたＩＴ統制上の問題について、おおよそ、全国各社で図３のような指摘が挙げられてきている。

図３に挙げた中では、よくある課題として、ログ管理の不備や問題が各社で見受けられる。多くの企業でログの取得程度はできていても、なかなか、ログの管理、つまり、ログに関わるＰＤＣＡサイクルを回すに至っていないのが現状である。

つまり、それは単なるログの取りっぱなしであり、あるポリシー（ＰＤＣＡのＰに当たる）に対して、何がいつどういった状態で問題があるか、又は、問題がないのかについて、早期発見・早期是正（ＰＤＣＡのＣとＡ）ができていない企業が多いのである。

そこで、まっとうな企業では、ログ管理を実践できるように、従来型のＩＴパッケージを購入して対応すべきと内部監査部門が指摘したり、ＩＴ部門が主体的に対応しようと試みたりするのであるが、問題は従来型のＩＴパッケージでＩＴ統制の課題克服を目指す際の多額なコストである（図４参照）。

ログ管理を従来型のＩＴベンダーに依頼して行う場合、まず、ログ管理を行うサーバー

＜図３＞全国各社でよく見受けられる監査法人からのＩＴ統制の監査指摘

・IT全般統制
- ID管理（幽霊IDにはご注意を）、アクセス管理の徹底
- 特権ユーザーIDの管理
- 発見的統制としての重点的ログ管理の徹底
- システム不正利用に関する管理体制　・職務分掌
- 変更管理　・障害時のバックアップ体制（BCP/BCM関連）
- 外部委託に対するSLA（サービスレベルアグリーメント）と監視体制
- トレーサビリティとレコードマネジメント（ログ・記録の保全）
- 監査証跡の一元管理(分散して保管して全体的に把握できない)
- 関連会社を含めた内部統制教育の不足　etc.

・IT業務処理統制
- 承認の際の履歴・記録不足　・二重入力のチェック漏れ
- 承認ステップが不足して十分な承認行為とみなされない
- 売上計上などの決算プロセスの属人性が高く、対応がバラバラ
- 突合/照合の漏れ　etc.

を自社内に設置し、そこに、ログの取得ツールを導入した上で、ログ管理に至るためのログ分析ツールを購入して使用することになる。

この重要なＩＴ統制上の課題対応１つだけでも、図４のとおり、従来型のＩＴ統制対応では多額の予算が必要であることがわかる。

一方、クラウドを活用し、現行の不十分で必ずしも健全であると立証できていないＩＴ統制対応を是正する、つまり、クラウド統制を行うことによって、１つのＩＴ統制上の監査指摘への対応で予算が２ケタ程度で済むこともわかる。

広範に求められるＩＴ統制上の課題克服に、クラウド統制が予算的にも実効性でも役に立つのである。

2.「クラウド＝危険」は妥当な判断か？

多くの企業が、図３で挙げた各ＩＴ統制上の課題克服に数億円の予算を簡単に確保できない実態がある。

そのような状況下で、予算がないからＩＴ統制が不十分でも良い、という暴論は通じないのは自明である。

ここで、クラウドを危険視する専門家も多いが、そもそも、「クラウド＝危険」「自社内のＩＴ（オンプレミス）＝安全」という、実態に沿わない非論理的でクラウドにとってアンフェアな議論や感情的判断に終始することが重要なのではないことも自明だ。

筆者としても、確かに、「クラウドは100％安全か（セキュアか）？」と問われれば、即答でＮＯと答える。しかし、重要なのは、既存のＩＴ環境やＩＴ運用がクラウドの危険性以上に問題をはらんでいるということだ。

ここで、筆者が監査の同行・現場指導で発見した某大手企業のＩＴ統制上の重大な問題が、この点を考える好例であるので図５に挙げておこう。

図５においては、ＩＴ統制やセキュリティの基本中の基本ともいえるサーバールームの入退室管理とそのログ管理（この場合、帳票というログ）が問題であった。

入室申請に対し、入室承認があって初めて入室できる規程であり、また、退室申請に対し、退室承認があって初めて退室できるものという説明を本社の会議室で内部監査人から聞かされていた。

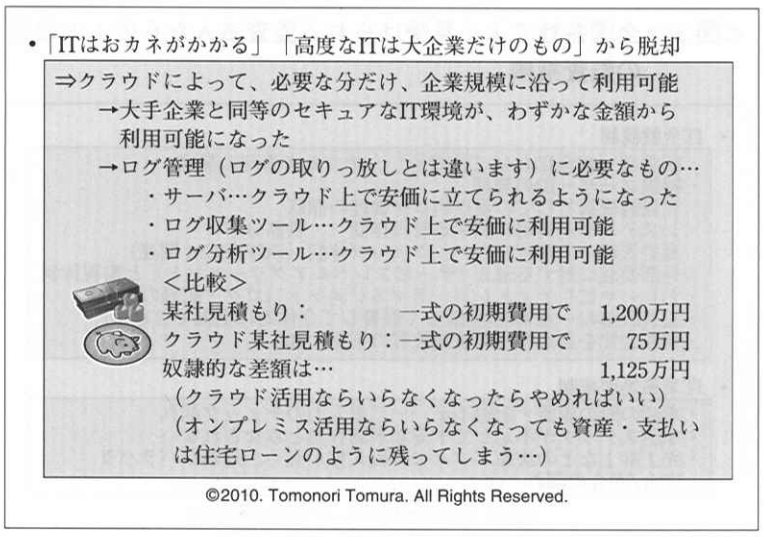
筆者は現場主義であるため、実際に現場を見せていただくと、図５のように入室申請と退室申請だけがあり、いずれの承認もない、つまり、勝手にサーバールームに出入りしている状態が放置されていた。

その未承認行為が続いていた期間は、承認者が出張で不在だったとのことで、承認者の代理権者の設定もなされないままであった。

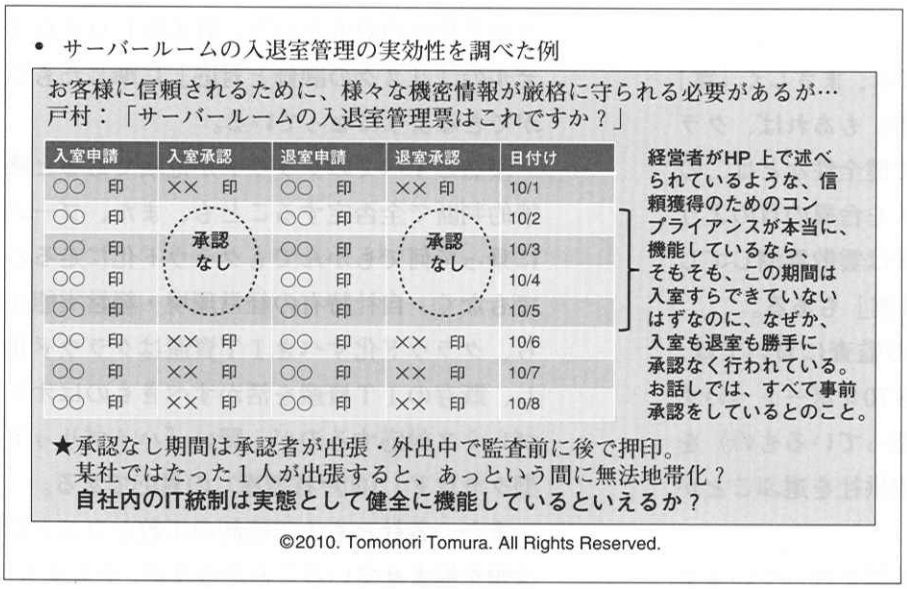
更に悪いことに、内部監査が往査に来る前には、つじつま合わせとして、承認印を後で押したとはバレにくいよう、承認印のハンコの向きを多少左右にずらしながら押し、帳票上は統制が効いていたように偽装して監査をパスしていたことがわかった。

この図５の例に出した部署は、

＜図４＞ログ管理１つをとって見ても多額な予算が必要になる例



＜図５＞ある大手企業のＩＴ統制上の「重大な欠陥」とＪ－ＳＯＸ偽装状態の例



ＪーＳＯＸでも通常の内部監査でも問題なしとして監査をパスしており、もはや、自社内のＩＴ活用（オンプレミス）では基本すらできていないＪ－ＳＯＸ偽装・監査偽装状態のＩＴ統制を行っていたといわれても仕方がない。

３．過剰なクラウド危険論という名のリスク

このように、既存の自社内のＩＴ（オンプレミス）に関わるＩＴ統制が崩壊している中で、果たして、クラウドの危険性を過剰に騒ぎ立て、既存のＩＴパッケージの導入にコストがかかり予算が得られないことを勝手な理由として、いっこうに自社のＩＴ統制の健全性・実効性を高めないでいることが許されて良いのであろうか。

クラウドは100％安全ではないが、既存のＩＴも100％安全なものなどあり得ない。ましてや、情報漏洩の事件・事故の大半は社内犯による漏洩だ。

クラウドという第三者（サードパーティー）は、自社からはある意味で独立的・客観的存在であり、自社より遥かに改ざんリスクや恣意性のリスクが少ないと見なし得る。

また、クラウド提供社側で問題が起これば、社内の甘い処分で済まされるものではなく、訴訟問題になり得るため、クラウド提供社側は、読者諸氏の自社内のＩＴ部門より遥かに健全性・遵法性などに力を注いでサービスを提供するのである。

予算がなくても、また、社内犯の情報漏洩に怯えなくても、クラウドで提供されるソフトやサービスを用いることで、より堅牢かつ健全なＩＴ統制が得られるのだ。

自社内にＩＴ資産（機器・ソフト・メンテナンス要員など）を備えることにこだわり過ぎない方が良いと筆者は考えている。

むしろ、クラウドを活用してＩＴ統制を負担なく強化する「クラウド統制」を進める方が、遥かに現実的で健全にＩＴ環境を整備・運用保守しやすいのである。

筆者は何も、クラウドのブームに便乗してクラウド推進派になっているのではない。ＩＴ統制の現状を全国各社で目の当たりにして、もはや、既存のＩＴ統制対応の仕方では限界があると痛感させられたとともに、クラウドに活路を見出すことで、閉そく状態を打破すべきだと訴えているのである。

〔３〕クラウド統制と監査

ここまでクラウドについての概要と昨今のクラウド関連の議論を踏まえた内容についてふれてきた。ここからは、クラウド統制と監査について述べていく。

ＩＴ統制の負荷軽減とＪ－ＳＯＸ監査を実効性・実態を伴ってパスすることを目的とし

ているクラウド統制では、そのキーとなるのは18号監査報告書又はＳＡＳ70レポートである。

クラウド提供社といっても、まさしく「雲」には安定的で健全な「羊雲」もあれば、クラウドブームに乗じるだけで健全性などは二の次としてクラウドサービスを台風の目のように注目を浴びて提供し、後は雲散霧消してしまう「積乱雲」のような「雲」もある。

内部統制・Ｊ－ＳＯＸの監査においては、18号監査報告書又はＳＡＳ70レポート（いずれも整備と運用の両面が整っているもの）を出せるクラウドサービス提供社を選ぶことが重要だ。

そうすれば、クラウド統制を行っている上では、基本的に、自社のＩＴ統制対応はクラウド提供社から18号監査報告書やＳＡＳ70レポートを取り寄せるだけで完了してしまうといっても良い。

更に、自社内のＩＴ資産をクラウド化におけるリスクの重要度を勘案しながら、順次、クラウド化していくのが妙策である。

1．クラウド化リスクマッピング記述書

この点は、筆者提唱の図６に示す「クラウド化リスクマッピング記述書」に沿って、リスクの重要度の低いＩＴ資産からクラウド化していけば良い。

図６では、読者諸氏には見なれているであろうリスクマップ（又はヒートマップ）を筆者流にアレンジしている。

縦軸にはクラウド化に伴うリスクの重要度、横軸にはリスクの発生確率（頻度）ではなく、業務種別を据えている。

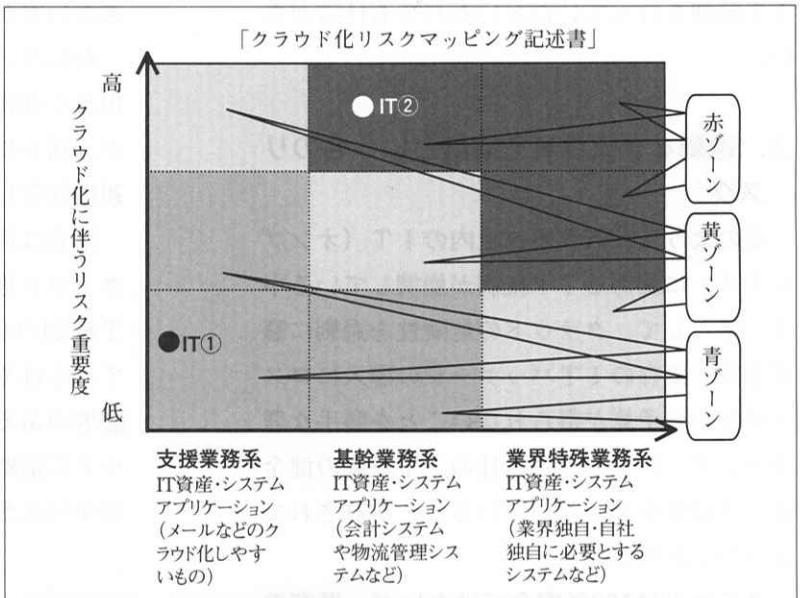
また、図６の上段のリスクマップでは、クラウド化に伴うリスクの評価、下段にプロットされた各ＩＴ資産におけるクラウド化への対応という、日本版ＣＯＳＯモデルの「リスクの評価と対応」に準じたものができるようになっている。

漠然とすべてのクラウドが危険であると感情的判断で全否定することも、また、ブームに乗って何でもかんでもクラウド化に走るのでもなく、自社特有の経営環境・経営実態から、クラウド化すべきＩＴ資産はクラウド化し、既存のＩＴ資産を活かすべきものはオンプレミス対応するのが、賢い「ハイブリッド型クラウド」（®戸村智憲）の対応である。

また、各社ともＩＴ統制の工数とコストには頭を悩ませていることだろうが、そもそも、ＩＴ資産が自社内にあるからこそ、ＩＴ統制対応が高負荷になるのである。

いっそ、健全で18号監査報告書あるいはＳ

＜図６＞クラウド化リスクマッピング記述書©戸村智憲



#	IT資産項目名	クラウド化におけるリスクの評価と対応	クラウド化判定とクラウド化の効果
IT①	メールシステム	定量・定性的リスク低	G-mailにて既存のものを置きかえて低コスト化
IT②	○○基幹システム	現状ではクラウド化移行時にデータ連携が困難で運用上の支障が想定される	パブリック・クラウド化は見合わせ、社内で統合・共通化可能な基盤にてプライベート・クラウドで効率化
…	…	…	…

ＡＳ70レポートを出せるクラウド提供社にＩＴを業務委託するクラウド統制に転じる方が、工数・コストの削減やサードパーティーによる独立的・客観的なＩＴ運用による健全性を高めやすいであろう。

ただ、留意すべき点は、18号監査報告書及びＳＡＳ70レポートに関する課題と誤解である。

まず、両者ともAgreed Uponであるがゆえに、異なる監査法人から業務委託先の内部統制の有効性を認めないという反応があることだ。

18号監査報告書もＳＡＳ70レポートも、その存在意義が脅かされるような監査法人の反応はあるべきではないと筆者は考えているが、実態としても、また、監査法人の儲けたい心理からも、すべてのケースに両者が監査において有効とは限らない点は留意いただきたい。

また、昨今、勝手に誤った解釈で「18号監査報告書を取っていれば業務委託先のセキュリティ監査もパスできる」ということを述べる者もいる。

この誤解を解いておくために、同じ「監査」といっても、Ｊ－ＳＯＸにおける「内部統制監査」と「ＩＴセキュリティ監査」の違いを、日本版ＣＯＳＯモデルを横倒しにしてカバー範囲を示してみた筆者オリジナルモデルで図７に示しておく。

図７に示したように、Ｊ－ＳＯＸの内部統制監査に関わる18号監査報告書やＳＡＳ70レポートは、そのカバー範囲がＩＴセキュリティ監査とは異なる点に注意しておく必要がある。

こういった点を理解しておいた上で、うまくクラウドとシンクライアント（ＰＣ端末に記憶装置（ハードディスクなど）がないもの）を組み合わせれば、極端な話、自社内で行う主なＩＴへの対応は、①アクセス管理、②ログ管理、③ＩＤ管理、④ＩＴ教育という４つ程度に絞ることも可能であろう。

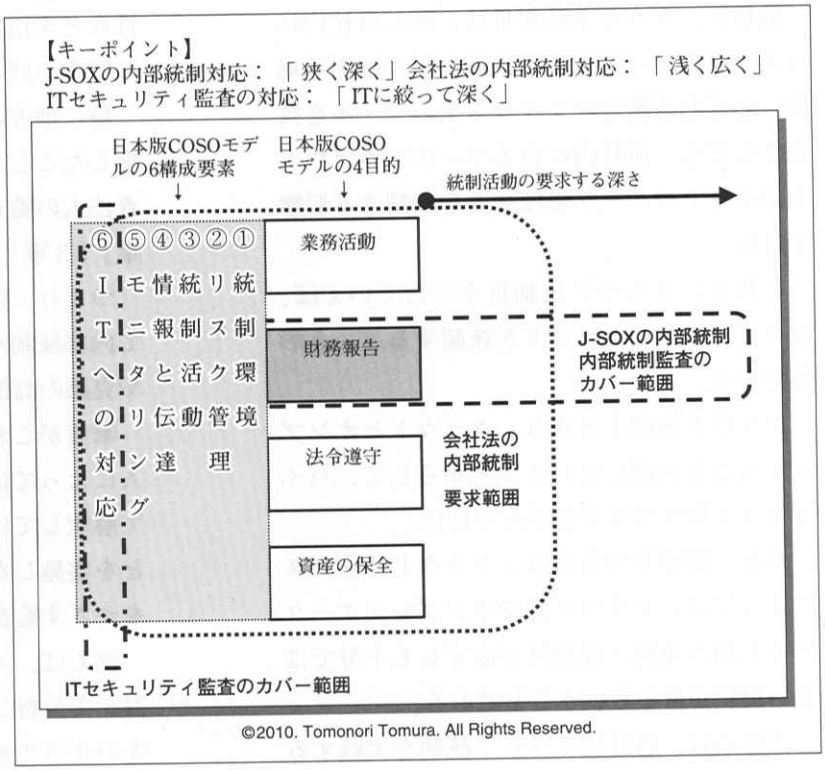
2．クラウド統制類型とクラウド統制記述書

さて、クラウド統制には、筆者の類型として３類型あるが、それらについて簡単に図８においてふれておくことにする。

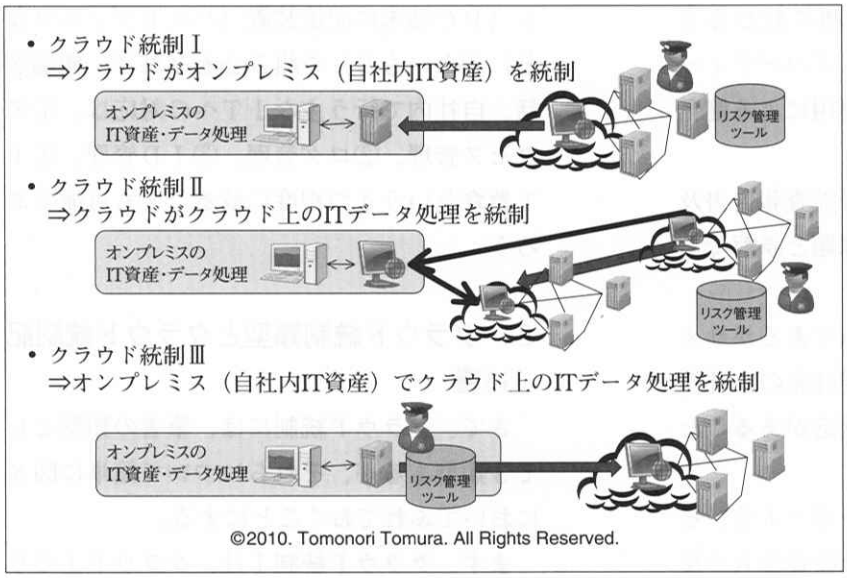
まず、クラウド統制Ⅰは、クラウド上のリスク管理ツール・ＩＴ統制ツールで自社内のＩＴ資産を統制する形態である。新たにＩＴ統制対応のツールを自社で高い初期費用やランニングコストを払わなくても、クラウド統制のサービスやツールを利用していけば、安く負荷も低い状態をもたらし得る。

一言でいえば、クラウド統制Ⅰは、クラウドがオンプレミス（自社内で開発・整備・運

＜図７＞内部統制監査とセキュリティ監査のカバー範囲の違い



＜図８＞クラウド統制の３類型



用しているＩＴ資産）を統制する形態である。

次に、クラウド統制Ⅱは、企業のクラウド活用が進んだ際に、クラウドにあるデータやデータ処理などを、クラウド上のリスク管理ツール・ＩＴ統制ツールで統制する形態である。

これも、クラウド統制Ⅱを一言でいえば、クラウドがクラウドを統制するという形態である。

最後に、クラウド統制Ⅲは、既に自社内にリスク管理ツール・ＩＴ統制ツールがある場合、わざわざ新たにクラウド上のツールを買わなくても、自社内にあるツールでクラウド上のデータやデータ処理などを統制する形態である。

これも、クラウド統制Ⅲを一言でいえば、オンプレミスがクラウドを統制するという形態である。

クラウド統制ⅠとⅢは、クラウドとオンプレミスとを併用していることからして、ハイブリッド型クラウドと呼んで良い。

ただ、留意すべき点は、クラウドサービスによっては、クラウド間やオンプレミス―クラウド間の連携・互換性が必ずしも十分ではない現状があるということである。

この点は、各社でクラウド統制を実践する際に、あらかじめ導入するクラウドを吟味しておいていただきたい。

次に、Ｊ－ＳＯＸにおける内部統制監査の対応として、監査法人に提示して協議する上での筆者オリジナルのクラウド統制記述書をご紹介しておこう。

ただ、その前に、全国各社の内部監査部門や内部統制推進部門やＩＴ部門などで見られた監査法人との「協議」に関する誤解を解いておこう。

多くの企業の監査に関わる現場では、往々にして、監査法人との「協議」の場が、監査法人の言いなりになる場になっている点に注意が必要である。

実施基準にあるＪ－ＳＯＸにおける監査法人との「協議」とは、現場や実務を知らない（あるいは知ろうとしない）監査法人の監査人に対し、しっかりと自社の実態や現場の特性などを伝えて「説得する場」であり「落とし所をつける場」であるということだ。

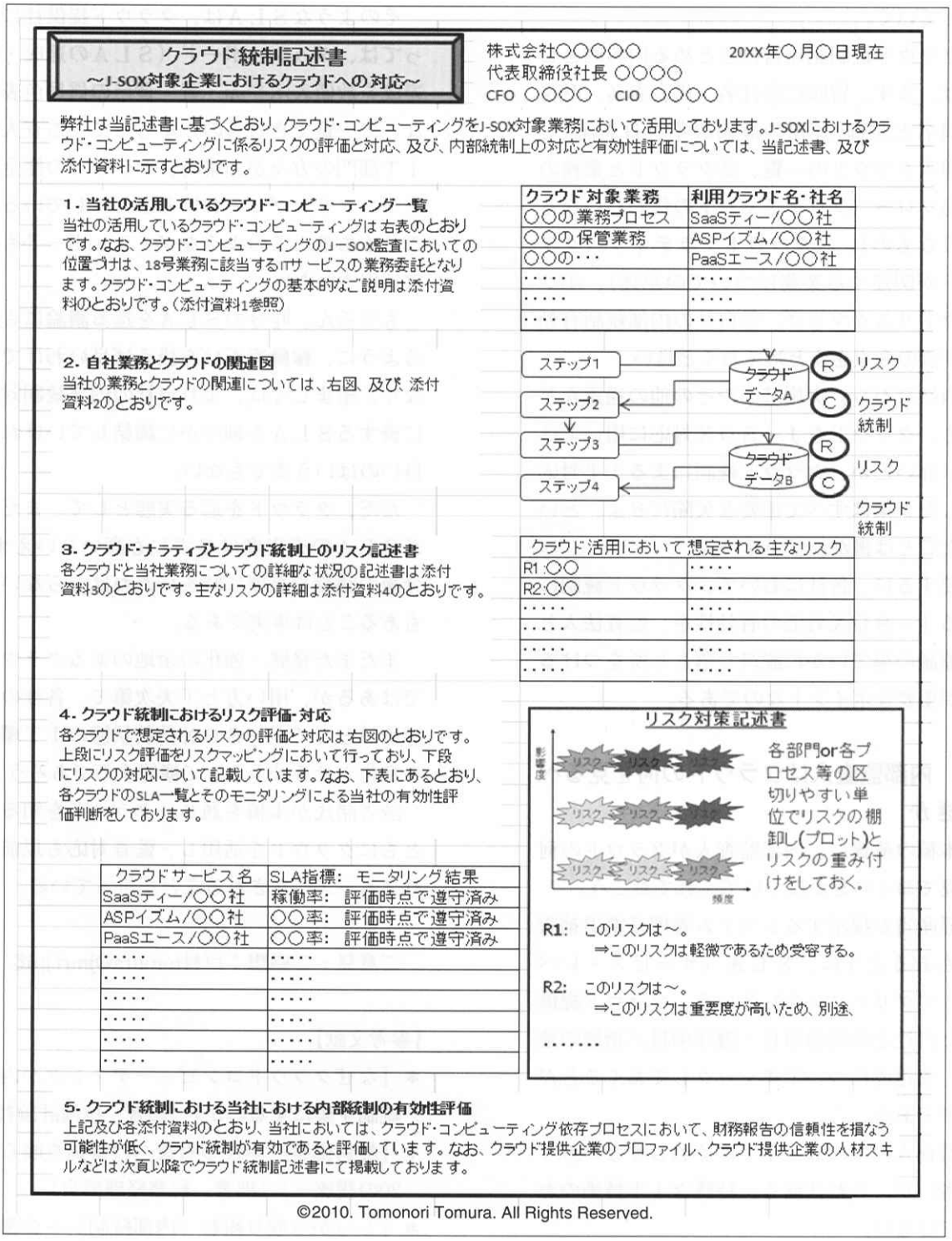
特に地方の上場企業各社を指導していて実感したことだが、地方の企業に回ってくる監査法人の監査人は、監査法人内のいわば「２軍」「３軍」の人材が多いということである。

つまり、監査法人といえど、監査人によって内部統制や監査の在り方についてのレベルや見識の高低にばらつきがあるのだ。

筆者がこれまで対してきた監査法人の監査人によっては、内部統制や実施基準等を誤って解釈している者や、現実的にはできないことを実施しなければならないと、机上の空論をかざす監査人も少なからずいた。

例えば、メインフレームのログをすべて取得して分析しろ、と言ってきたり、業務委託先のすべてを監査できる監査権を取得する業

＜図８＞クラウドの監査報告書としての「クラウド統制記述書」©戸村智憲



クラウド統制記述書
～J-SOX対象企業におけるクラウドへの対応～

株式会社○○○○○　　20XX年○月○日現在
代表取締役社長 ○○○○
CFO ○○○○　CIO ○○○○

弊社は当記述書に基づくとおり、クラウド・コンピューティングをJ-SOX対象業務において活用しております。J-SOXにおけるクラウド・コンピューティングに係るリスクの評価と対応、及び、内部統制上の対応と有効性評価については、当記述書、及び添付資料に示すとおりです。

1. 当社の活用しているクラウド・コンピューティング一覧
当社の活用しているクラウド・コンピューティングは右表のとおりです。なお、クラウド・コンピューティングのJ-SOX監査においての位置づけは、18号業務に該当するITサービスの業務委託となります。クラウド・コンピューティングの基本的なご説明は添付資料のとおりです。（添付資料1参照）

クラウド対象業務	利用クラウド名・社名
○○の業務プロセス	SaaSティー/○○社
○○の保管業務	ASPイズム/○○社
○○の・・・	PaaSエース/○○社
・・・・・	・・・・・
・・・・・	・・・・・
・・・・・	・・・・・

2. 自社業務とクラウドの関連図
当社の業務とクラウドの関連については、右図、及び、添付資料2のとおりです。

3. クラウド・ナラティブとクラウド統制上のリスク記述書
各クラウドと当社業務についての詳細な状況の記述書は添付資料3のとおりです。主なリスクの詳細は添付資料4のとおりです。

クラウド活用において想定される主なリスク	
R1:○○	・・・・・
R2:○○	・・・・・
・・・・・	・・・・・
・・・・・	・・・・・
・・・・・	・・・・・
・・・・・	・・・・・

4. クラウド統制におけるリスク評価・対応
各クラウドで想定されるリスクの評価と対応は右図のとおりです。上段にリスク評価をリスクマッピングにおいて行っており、下段にリスクの対応について記載しています。なお、下表にあるとおり、各クラウドのSLA一覧とそのモニタリングによる当社の有効性評価判断をしております。

クラウドサービス名	SLA指標: モニタリング結果
SaaSティー/○○社	稼働率: 評価時点で遵守済み
ASPイズム/○○社	○○率: 評価時点で遵守済み
PaaSエース/○○社	○○率: 評価時点で遵守済み
・・・・・	・・・・・
・・・・・	・・・・・
・・・・・	・・・・・
・・・・・	・・・・・
・・・・・	・・・・・
・・・・・	・・・・・

5. クラウド統制における当社における内部統制の有効性評価
上記及び各添付資料のとおり、当社においては、クラウド・コンピューティング依存プロセスにおいて、財務報告の信頼性を損なう可能性が低く、クラウド統制が有効であると評価しています。なお、クラウド提供企業のプロファイル、クラウド提供企業の人材スキルなどは次頁以降でクラウド統制記述書にて掲載しております。

務委託契約にしろ（独立した第三者企業のノウハウなども丸裸にしろというに等しい）と言ってきたりする監査法人の監査人が少なからずいた。

こういったことを踏まえ、クラウド統制をもって内部統制監査をパスしやすいようにするために、協議における強力な説得材料の１つとして、クラウド統制記述書を図９にご紹介しておく。

図９では、Ａ３用紙の縦１枚に概要をまとめ、詳細な説明や説得材料が必要になる際には、そのサマリーとしてのＡ３用紙１枚の記

述書の後に、補足資料を添付していく形態をとっていく。

クラウド統制記述書にまとめる内容例としては、まず、冒頭に会社名、代表者名、財務役員名と整備/運用の評価の年月日を記し、①導入クラウドの一覧、②クラウドと業務の簡易フロー（フローチャートの代わりになるようなもの）、③クラウドナラティブ（クラウドが関連する業務についての記述）、④クラウドリスクマップ、⑤自社の内部統制有効性評価の５点をまとめておくと良い。

当然ながら、実施基準やその他の通達などでも、クラウドをＪ－ＳＯＸ対応に用いてはいけないとか、クラウド統制によるＩＴ対応をした企業はすべて重要な欠陥にせよ、といったことは書かれていない。

要するに、各社において、クラウド統制によるＪ－ＳＯＸ対応の有効性を、監査法人との協議の場でいかに説得し落とし所をつけるかが重要なポイントなのである。

3．内部監査人はクラウドの何を見るべきか

本稿の最後に、内部監査人がクラウドの何を見ておくべきかについてふれておこう。

経産省が提示するシステム管理基準追補版にもあるように、ＳＬＡ（サービス・レベル・アグリーメント）という、クラウド提供社と自社との契約項目・遵守項目／指標の達成・未達成についてチェックしておくことが必要である。

監査人の中には、ＩＴにくわしくない方々も多いが、これは何も、特殊なＩＴ技術のお話ではない。

例えば、「稼働率○%」というＳＬＡがあれば、それがクラウド提供社から自社に対して遵守されているかをモニタリングしておくことで済むであろう。

そのようなＳＬＡは、クラウド提供社によっては、ダッシュボード（ＳＬＡの達成・未達成を数値表示や赤・青・黄色の信号色表示などで一覧できるもの）をもって、監査人やＩＴ部門の方々が、常時、クラウドの健全性をモニタリングしておけるようにしているところもある。このようなダッシュボードも適宜活用されたい。

もちろん、昨今のＳＬＡを巡る議論にもあるように、稼働率だけを扱えば良いわけではなく、望ましくは、より自社の内部統制対応に資するＳＬＡを細やかに締結していければ良いのはいうまでもない。

ただ、クラウドを巡る実態として、まだまだＳＬＡの充実度は必ずしも高いといえず、今後の議論や発展に時を待たねばならない面もあることは事実である。

まだまだ発展・強化の余地のあるクラウドではあるが、用い方と工夫次第で、各社の旧態依然としてＪ－ＳＯＸ偽装状態のＩＴ環境を良化させる妙手として機能するであろう。

読者諸氏が本稿を通じ、クラウドを知るとともにクラウドを活用し、監査対応も以前よりスムーズになされることを祈っている。

ご意見・ご感想：戸村tomura@jmri.jp迄

【参考文献】

＊『なぜクラウドコンピューティングが内部統制を楽にするのか』（拙著、技術評論社）
＊『経営偽装～不祥事対策への警鐘を鳴らす20の視座～』（拙著、税務経理協会）
＊『しっかり取り組む「内部統制」～企業健全化プログラムと実践ノウハウ～』（拙著、実務教育出版）