

J-SOX クラウド・パーク構想： IT 統制からクラウド統制へ ～クラウド化による J-SOX 対応コストの極小化～



J-SOX クラウド・パーク構想

J-SOX クラウド・パーク構想とは、最近、やっと話題となって認識が広まってきたクラウドコンピューティングを活用することで、J-SOX 対応コスト・工数・人員などを一気に削減していこうという構想である。基本的に現状の J-SOX 対応に関しては、既存の IT システムを使って、いわゆるオンプレミス（自社内に IT 資産を保有している）の状態ですerverを持っていたり、サーバールームを社内に備えていたりする状態である。あるいは、一部をデータセンターのような形で外部委託しているわけだ。現状では、社内で IT 資産を持っていることで、社内の一つ一つに関して事細かに IT 統制を行わなければいけないことが J-SOX 対応負荷の最大のネックとなっている。受注から発送に至るまで、売上計上、また、財務報告を取りまとめる全般において、財務報告を歪めかねない問題がないかを事細かに、改ざんリスクの視点から監査法人の視点で事細かにやらなければいけない状態である。これにもものすごく手間がかかるし、また、それに関わる IT 統制の活動に関して非常に負荷が大きい。

そこで、いっそのこと、IT に関してはオンプレミスでの資産保有をやめてしまって、一気にクラウド化してしまった方がいいのではないか、という考えを J-SOX 負荷軽減において持っているのである。特にデータセンターという形では、従来型の監査から見れば、監査法人としては 18 号業務に該当する業務委託であるという見方をされる。そのような場合には、18 号監査報告書や SAS70 レポートがなければ、各アウトソース先・業務委託先に向いて行って、自社のやり方で委託先のすべてチェックをしていくことになる。自社の J-SOX 対応のやり方に合わせさせる、という形にしていかなければならないということになってしまうのである。もしくは、非常にやりやすいパターンとしては、SAS70 レポート、あるいは、18 号監査報告書というアウトソース先として J-SOX 監査をクリアできる状態であるというレポートを出してもらおうかということになる。新規で外部委託先に 18 号監査報告書か SAS70 レポートを取得させるにしても、自社に合わせた J-SOX 対応させるにしても、非常に金銭面でも工数面でも負荷が大きいのが悩みどころである。ましてや、自社の IT 子会社に委託したとしても、その IT 子会社を含めて一体として高負荷の J-SOX 対応を行わなければならないになってしまうのである。

逆に言えば、この SAS70 の報告書、もしくは、18 号監査報告書を出せるクラウド・ベンダーで企業に必要な IT 環境をワンストップで整え、そこに企業から IT 環境を全て外部委託してしまった方がかえって安くつくはずである。つまり、自社に極限まで IT 資産を持っていない状態であれば、アクセス管理・特権ユーザ管理・ログ管理と IT 教育以外は、自社内および自社グループ内で IT 統制の高負荷な対応をしなくても、SAS70 レポートまたは 18 号監査報告書で全てを代行してしまえるといっても過言ではない。クラウド・コンピュ

ーティングによって、メンテナンスの手間もコストもバージョンアップごとにアップグレードや買い換えする費用負担が必要なくなるのである。なぜなら、それらはクラウド・ベンダー側で全て行うからである。オンプレミスでの対応よりも負荷が低減すると共に、これまで IT 部門が担当させられていた雑多な仕事なく、より IT 戦略と効率化の仕事に専念できるようになるのである。しかも、クラウド・ベンダー側では、優秀な人材を集約的に集めてサービス提供していることが多く、自社内人材よりはるかに高レベルの統制環境をクラウド側で整えられる可能性も高い。つまり、メンテナンスのような戦略性の低い作業に、自社内で高度なレベルの人材を充てなくても、それ以上のレベルの人材でクラウド側において対応できるようにしてしまえば良いのである。

そもそも、自社内の IT 環境がリスクに満ちている現状を鑑みる

ちょっと考えてみてほしい。自社内に高コスト・高負荷の状態を甘受して、素晴らしいサーバールームを備えている企業もあるが、多くは、サーバールームが自社内であるが故に、いい加減な対応が見られないだろうか。入退室管理ひとつとってみても、入室/退室申請と入室/退室承認が必要な帳面で管理している企業もある。この企業で、筆者が実際に現場視察で目の当たりにしたのは、大手グループ企業の IT 環境であっても、入室申請と退室申請だけの 1 週間分のハンコが並んでいて、入室も退室も承認印がひとつもなかった。つまり、この 1 週間では、基本的に誰も入室申請を承認されていないため、誰も退室申請と退室する人のハンコは押せないはずである。結局明らかになったのは、承認者が 1 週間出張していたため、承認者に断りなく入退室していて、後でつじつま合わせのように、承認者が申請内容や稼働状況をチェックすることなく、承認のハンコを押してサーバールームへの入退室管理ができていくかのように形式だけ整えていたのである。もちろん、入退室カードで入退室管理をしている企業も多いが、そのカードを入室権限のない者にまで貸し借りしている企業もある。

つまり、IT 環境の中枢部であるサーバールームがこのありさまである状態で、クラウド側にデータを保管するリスクを抱いているようなことは異常なのではないかということだ。オンプレミスでの IT 環境のチェック&モニタリングと是正活動が形式だけであるのが現状なら、IT 資産を自社内で持っている状態よりも、クラウド・ベンダーに任せる方がよほど健全な IT 環境を保てるのではないか。定期レポートやサービス・ヘルス・ダッシュボードや SLA などによるチェック&モニタリングや、その分析結果からクラウド・ベンダー側に是正させることができるからである。クラウド・ベンダー側にとってみれば、クラウドのサービス提供上の契約違反や訴訟問題になるため、自社内で IT 環境を整える自社内の人材より、IT の健全性にかけるモチベーションも素早さも正確さなどの確保に必死になるのである。

却って安心できる状況でクラウド側に委託することで、自社内に抱えなければならない「雑多な業務に費やされる高度な IT 人材」は不要になり、J-SOX 対応工数もコストも、

SAS70 レポートや 18 号監査報告書で代用することで、これまで IT 統制で悩んできた負荷が大幅に下がるということになるのである。クラウド・コンピューティングというものが整ってきたおかげで、それだけの思い切った対策、つまり、これが筆者の述べる「クラウド統制」(IT 統制のドラスティックな進化形)を行えるようなことになるのである。クラウド統制が十分に整えば、海外子会社であっても基本的にクラウド上では、IT 環境が統一されやすいため、海外子会社の J-SOX 対策においてもクラウド統制として各国の各事業拠点で個別に IT 環境を整えなくても、クラウド・ベンダーの方に全部委託してしまうことによって、わざわざ現地の IT 統制を事細かに、文化の違い、言葉の違い等を無理やり統一させなくても、低コスト・低負荷で IT 全社統制上もうまく対応することができるようになるのである。単に、上場している親会社だけではなく、持ち株会社から子会社、関連会社に至るまで、全てクラウド化による SAS0 レポートや 18 号監査報告書を出せるクラウド・ベンダー最大限に活用したクラウド統制を行うことによって、これまでは想像できなかったような対応工数の大幅な削減が可能になる。これは、短期的な収益改善に寄与する可能性のあるリストラよりも、運用コストを含めた長期的な財務体質改善に遥かに大きな寄与をするものである。

IT 統制から「クラウド統制」への転換

筆者が日本初 (おそらく世界でも初) で提唱した「クラウド統制」(参照: 共同通信 PR ワイヤー<http://prw.kyodonews.jp/press/release.do?r=200903281921>) においては、これまでのオンプレミス・ベースの従来型の IT 統制から飛躍的に効果性・効率性が高まる。クラウド統制上では、J-SOX 対応に必要なデータのバックアップもクラウド側で行われる。又、何かの障害、故障、災害などの、新会社法施行規則第 100 条における損失等のリスクがあった場合でも、データを確実に保管し、保管することに加え、クラウド側のデータ保管場所の分散やクライシス体制の整備により、危機下にあっても継続性を持って保管したデータをリストアできるようになるのである。オンプレミス・ベースであれば、自社がデータを 2 か所に保存し、地震や火災などの対策にあたらなければならないため、非常に負荷が高いことになる。又、これまでそうした対応をとっていた企業では、非効率な IT 投資を知らずか行っていて「隠れた IT コスト」を垂れ流していることになるのである。これは何も J-SOX 対象企業だけではなくて、クラウド統制がカバーできる内部統制の中で、新会社法における中堅中小企業の内部統制の IT 対策も、J-SOX 対象企業と同様に低コスト・低負荷で対応できるようになるのである。特に、中堅中小企業にとっては、IT 資産は大手企業との間に資本の壁がある。バックアップ体制をとれる IT 資産を、自社内に確立するには、資金面でも人材面でもあまりにも障壁が高いのである。その意味で、クラウド統制とは、中堅中小企業の IT 資産の壁を取り払って、大手企業と遜色ないレベルのものを手に入れ、取引先やお客様からの信頼を勝ち得る資源を低価格で得たと言えるのである。その意味で、IT 資産による「身分制度」の解放宣言でもあり、IT における「不平等条約の解

消」のようなものでもある。

もちろん SAS70 レポートや 18 号監査報告書を取得するには、それなりにクラウド・ベンダーの企業規模が大きく資金的に余力がなければできないことでもある。3,000 万、あるいは、4,000 万円という SAS70 レポート、あるいは、18 号監査報告書の取得費用をカバーできないクラウド・ベンダーは、この点でクラウドの競合状態においてビハインドをとることになる。それではクラウドの魅力がそがれかねないし、中堅中小クラウド・ベンダーの育成につながらないため、筆者はクラウド統制記述書という形で、J-SOX 対象企業が中堅中小クラウド・ベンダー活用時における J-SOX 対応手法を提言している。これは、J-SOX 対象企業が監査法人との協議において、中堅中小クラウド・ベンダーでも健全な IT 環境を確保できることを監査法人に説得する材料となるものである。SAS70 レポートや 18 号監査報告書がなければならぬというわけではなくて、あればなお良いが、逆になければ、ほかの代替的な手法でクラウド・コンピューティングが監査に耐えうる安全性があり、財務報告の信頼性を脅かすようなものではないことを示せば良いのである。

また、クラウド統制のメリットとしては、第三者に業務委託している形態であるため、基本的にはオンプレミスの IT 資産を活用した際の IT 統制と比して、改ざんリスクが極めて低い、ということを経査法人さんに訴えかけることができるのである。要するに、クラウド統制においては、SAS70 レポートや 18 号監査報告書の提示、又は、クラウド統制記述書をまとめて、それを監査法人に提示して協議・説得していくということで監査対応していくのである。これによって、RCM(リスク・コントロール・マトリクス)で掲出したリスクとコントロールは全てテストしなければならないところを、テスト工数を一気に削減する狙いもあるのだ。当たり前のことであるが、J-SOX 対象企業は、上場を取りやめたり金融商品法が廃止になったりしない限りは、これから半永久的に続くのである。つまり、J-SOX 運用コストを下げなければ、どれだけ「ムダとり」や他の業務での経費削減を徹底していても、半永久的に J-SOX における高コスト体質が企業グループ全体の財務体質を悪化させ続けることになるのである。上場を維持しようとして行う J-SOX 対応にかかるコストが高すぎるままで、結果として、上場を維持できない財務体質の悪化で継続疑義や格付け低下等に起因し、上場廃止や上場し続けられ内というような経営のダメージが顕在化してしまうことも、決して絵空事ではないのである。IT 統制はクラウド統制に移行しなければ、高コスト体質を垂れ流す経営判断をし続けていることになってしまう危険性があるのである。つまり、非効率な状態で IT 資産を自社内に保有し続けることは、日本版 COSO モデルにおける内部統制の 4 つの目的で言うところの、業務活動の有効性・効率性を高めるという目的に反する状態になるのである。単に流行に乗って流されるのではなく、新たな潮流にあって、クラウド・コンピューティングを活用して内部統制を低コストで効率的に向上していくことに目を向けなければならない現状がある、ということなのだ。

(次ページに筆者略歴)

日本マネジメント総合研究所理事長 日本 ERM 経営協会会長
岡山大学大学院非常勤講師 (内部統制・ERM 担当)
公認不正検査士 戸村智憲
「J-SOX クラウドパーク構想」

【筆者略歴： 戸村智憲】日本マネジメント総合研究所 理事長 www.jmri.jp

早大卒。米国 MBA 修了 (全米でトップ 0.5%にのみ授与される全米優秀大学院生受賞)。国連勤務にて、国連内部監査業務ミッション・エキスパート、国連戦略立案ミッション・エキスパート・リーダーなどを担当。民間企業役員として内部監査業務の統括にもあたった。経営行動科学学会理事 (兼) 東日本研究部会長も務めた。2006 年 7 月 1 日の管理会計学会大会 (於：甲南大学) にて、世界初で収益戦略とリスク対策の PDCA サイクルを一元管理する ERM に基づく SRB スコアカード (第 4 世代バランス・スコアカード) を提唱。FBI 推奨の不正検査・監査・内部統制の専門資格である公認不正検査士 (CFE) を取得。内部統制を指導するコンサルタントや講師を指導する講師としても登壇。日本の人気講師ランキングで北野大(きたのまさる)教授と並びトップ 3 位にランクイン(日経産業新聞の特集記事にて)。日本マネジメント総合研究所理事長として、年間 120 講演に加え、コンサルティング、連載 9 本や書籍の執筆にもあたる。岡山大学大学院非常勤講師としても教鞭をとり、産学両面で活動中。日本初でクラウド・コンピューティングと内部統制の在り方を述べた「クラウド統制」を提唱。私費を投じた研究組織である日本 ERM 経営協会において、会長 (兼)『ERM レビュー』編集長を務めている。2009 年 4 月に一般書店流通型の機関誌『ERM レビューVol.1』創刊号を出版し、Vol.2 にてクラウド特集に取り組んでいる。BS 朝日『賢者の選択』にて内部統制の専門家として TV 出演。NHK 総合の世直しバラエティー番組『カンゴロンゴ』のコンテンツ提供・番組制作監修も行う。代表作として『リスク過敏の内部統制はこう変える!』(出版文化社) など多数。

内部統制・コンプライアンス推進協会顧問、 (株)日本経営協会総合研究所 アドバイザー

(社)日本取締役協会会員、 組織学会学会員、 産業・組織心理学会学会員

日本人材マネジメント協会正会員、 (株)メイツ エグゼクティブ・アドバイザー

米国連邦航空局自家用パイロット、 第一級小型船舶操縦士

BCIJA メンバー： BCP/BCM 普及啓発と COSO-ERM 経営実現へ

【クラウドへの取り組み】

クラウドのリスク・課題を見つめ、内部統制上・セキュリティ上の不安なくクラウドの健全な普及啓発に向けて活動中。

戸村が会長を務める日本 ERM 経営協会にて、下記のクラウド特設セミナーを開催予定。

- ・ 2009 年 5 月 22 日(金)19:00～ 富士ソフト様ご登壇にて「クラウドの現状と課題」
- ・ 2009 年 7 月 31 日(金)19:00～ セールスフォース・ドットコム様ご登壇で「クラウド統制」

詳細： <http://prw.kyodonews.jp/open/release.do?r=200904202347>

『ERM レビューVol.2』(2009 年 9 月頃出版予定)にて、クラウド特集として、セールスフォース・ドットコム様、富士ソフト様、KDDI 様などをはじめ、米国のクラウド状況だけではなく日本におけるクラウドの展開について見つめる対談記事を掲載予定。

日本 ERM 経営協会について：www.j-erm.org