

クラウド, iPhoneなど話題の最新技術を満載!

ITエンジニア必携スキルが身に付く技術情報誌

Software Design

ソフトウェア デザイン

2009年9月18日発行 毎月1回18日発行 通巻293号(発刊227号)
1985年7月1日第三種郵便物認可 ISSN 0916-6297

2009
September

9

チャレンジしてみませんか?

特集

知りたい!

試したい!

クラウド コンピューティング

Amazon EC2/S3

MapReduceとHadoop

クラウドと法



特別付録
小冊子



iPhone開発 AtoZ

iPhone OS 3.0 対応

オープンソースを使っていますか?
OSC 2009 Kansai

緊急レポート!
VirtualBOX 3.0登場

新連載 あなたは知っていますか? OSの隠れプロセス

第2特集

Webアクセスの
高速化宣言

極めるSquid

IT 統制は「クラウド統制」へ ——ハイブリッド型クラウドによる 賢い内部統制対策

クラウドコンピューティングを現実企業システムとして使うにあたり、いろいろな問題が考えられます。まずデータの保全です。自社で持つのか、それともすべてクラウド側に預けてしまうのか? 大きな問題です。筆者はその解答として、ハイブリッド型クラウドによる解決を提唱します。銀行にお金を預けるかのようにデータを預ける、このたとえをベースに、企業におけるIT 統制を考えます。そして、中小企業におけるクラウド導入のメリットを示します。

TEXT BY 日本マネジメント総合研究所 [info@jmri.jp] 理事長 戸村智憲 (TOMURA, Tomonori)

J-SOX 初年度で問われた IT 統制項目



J-SOX への対応は必須

新会社法と J-SOX (金融商品取引法) を契機に、IT 面における内部統制対応として IT 統制が重点課題となっています。

新会社法では、従業員が 2 人以上いるすべての会社で「健全に儲け続けるためのしくみ」としての内部統制を充実させる必要があります。また、J-SOX では、上場企業/グループ会社/関連会社や、重要な業務委託先に至るまで、高度な IT 統制が求められます。クラウドが企業の IT 環境にかかわりを持つ昨今、クラウドは内部統制においてどのように扱われるべきかについて、十分検討しなければなりません。



IT 統制とは何か?

◆ IT 統制の要求事項

筆者は日本でもかなり初期から、全国で内部統制の指導をしてきました。その中で見受けられた、各社共通に監査法人から指摘を受けた IT 統制の要求事項を、表 4.1 にまとめました。

IT 統制は、次ページ表 4.2 のように、3 つの区分に分けられます。グループ全体で整合性を求める IT 全社統制、次に、個々の企業でセキュア

な IT 環境を構築する IT 全般統制、最後に、個々の企業で、諸業務を正確に処理するための IT 業務処理統制の 3 つの対応が必要です。その中で、監査法人からの重点指摘項目は、IT 全般統制と IT 業務処理統制です。

◆ 監査の限界から「クラウド統制」へ

表 4.1 の各要求事項を、従来のパッケージソフトやシステム構築で IT 統制対応しようとする、初期費用もメンテナンス費用も、運用保守の IT 要員の確保も、企業経営を非常に圧迫する重荷となります。また、オンプレミス (自社内での IT 資産保有) での対応では、自社が改ざんや恣意的な操作を行えるため、監査の指摘が非常に厳しく

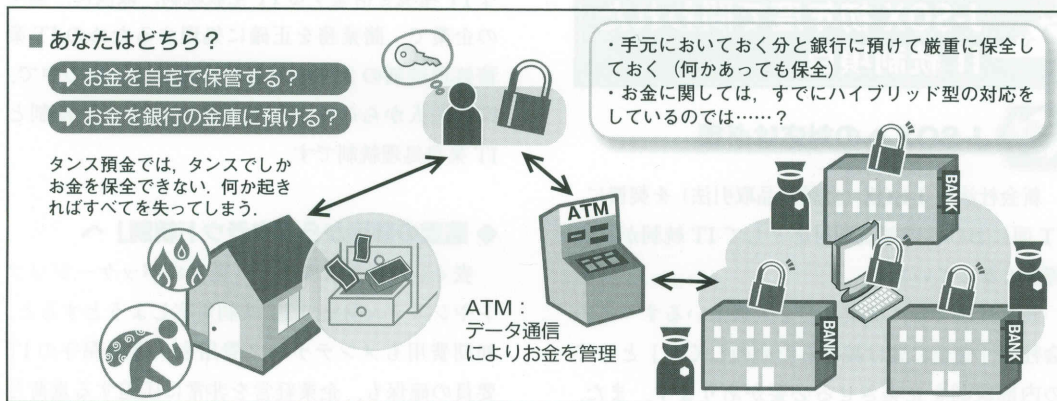
▼表 4.1 監査法人からの指摘例

全般統制	・ ID 管理 (幽霊 ID には注意)、アクセス管理の徹底
	・ 特権ユーザ 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 (分散して全体を記録できない)
業務処理統制	・ 関連会社を含めた内部統制教育の不足 etc.
	・ 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/計上等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.

▼表 4.2 IT 統制ひとまとめ（参考『システム管理基準 追補版』経済産業省）

IT 統制の種類	目的	統制項目
IT 全社統制	企業集団全体の IT を健全に維持／監督するために構築する。内部統制の基本的要素に対する IT の統制方針と統制	a. IT に関する基本方針の作成と明示（統制環境）
		b. IT に関するリスクの評価と対応（リスクの評価と対応）
		c. 統制手続きの整備と周知（統制活動）
		d. 情報の伝達の体制としくみの構築（情報と伝達）
		e. 全社的な実施状況の確認（モニタリング）
IT 全般統制	財務報告に関連する業務プロセスにおける情報の信頼性を保証するための「プログラム」と「データ」の信頼性を確保するための統制	a. IT の開発／保守にかかわる管理（ソフトウェアの開発／調達、IT 基盤の構築、変更管理、テスト、開発／保守にかかわる手続きの策定と保守）
		b. システムの管理／運用（運用／管理、構成管理、データ管理）
		c. 組織内外からのアクセス管理等のシステムの安全を確保（情報セキュリティフレームワーク、アクセス管理等のセキュリティ対策、情報セキュリティインシデントの管理）
		d. 外部委託に関する契約の管理（外部委託先との契約、外部委託先とのサービスレベルの定義と管理）
IT 業務処理統制	IT において承認された業務が全て正確に処理／記録されることを確保するために業務プロセスに組み込まれた内部統制	a. 入力情報の信頼性を確保する統制
		b. 出力情報の信頼性を確保する統制
		c. データの維持管理信頼性を確保する統制
		d. EUC（エンドユーザコンピューティング：スプレッドシート（表計算ソフトウェア）など

▼図 4.1 データを外部に預ける不安……



なります。

そこで、筆者は、最大限にクラウドを活用して内部統制を充実させる「クラウド統制」を日本で初めて提唱しました。これまで業務委託先は、IT 統制上、自社以外にも内部統制を強いる厄介もの扱いでした。しかし、クラウド統制では、業務委託先を「改ざんリスク／恣意性なき第三者」として逆手にとる、逆転の発想で低コストの IT 統制を加速させるのです。

たとえば、IT 全般統制で強く求められるバックアップについては、自社内で物理的に 2 拠点にデータを分散して保存しなくても良くなります。クラウド統制ならば、自然とクラウド提供側が、データを改ざんリスクも恣意性もなく分散保存するため、監査で指摘される IT 統制対応を低コストで

満たせます。クラウドならば、オンプレミスで買収する固定資産ではないので、気に入らなければ別のクラウドに乗り換えやすいというメリットもあります。

クラウドへの不安は杞憂



タンス預金か銀行預金か？

皆さんの中には、データをクラウド上に預ける不安を感じる方が多いかもしれません。しかし、自社内でデータを管理することは、本当に安全なのでしょうか。

ここで質問です。皆さんは全財産をどう管理していますか。図 4.1 をご覧ください。タンス預金

ですか。それとも、銀行に預けますか。

自宅（オンプレミス）で全財産を持っていると、火事や盗難のリスクなどにつねに怯えていることになります。また、皆さんが銀行と同等の頑丈な金庫を持ち、屈強で信頼できる警備員を自費で雇い続け、日々セキュアにお金を管理するのは無理でしょう。札束が火事で焼けたり、泥棒に盗まれたりしたら、皆さんは全財産を一気に失うことになります。

一方、近くの ATM から、皆さんのお金を銀行に預けた場合を考えてみましょうか。ATM からセキュアなデータ通信でお金が A 支店に計上され、個々人が買うよりはるかに頑丈な金庫で現金が保管されます。



銀行はあたかもクラウド

銀行では、監視カメラもあれば、特別に訓練された警備員が、銀行強盗対策や火災対応を行います。万が一、A 支店で火事や銀行強盗があってもお金が盗まれても、銀行全体として皆様のお金は保全されます。銀行という多数の支店の集まり全体（クラウド）として、皆様の財産が守られているのです。銀行のシステムは、皆様が毎回バージョンアップ費用を払わなくても、銀行側がセキュアな管理システムを整備・更新・保守してくれるのです。

つまり、皆さんの大事な財産を預けている銀行は、構造的には、昔からある「銀行というクラウド」のようなものなのです。



クラウドにデータを預けたほうが安全

図 4.2 をご覧頂ければ、企業の実態に置き換えてクラウドにデータを預ける不安を解消できるのではないのでしょうか。自社内のサーバはどれくらい堅牢でしょうか。自社内のサーバールームに、入退室カードを勝手に貸し借りして出入りはありますか？ 各企業にいる IT 要員は、クラウド提供企業で特別に訓練され、多数の企業のデータ処理を経験する熟練人材より優秀ですか。多くの企業では、データを自社内より、むしろ、クラウドに預けたほうが安全なのです。

また、監査法人が、業務委託先として内部統制の適格性を証明する報告書を付与しているクラウド上では、これまでお金も人手もかけてやってきた、自社内での膨大な IT 統制対応が不要になります。運用保守でのバッチ処理も不要になります。監査において、そのようなクラウドはフリーパス状態となり、IT 統制対応の手間もコストも一気に削減できるのがクラウド統制の良さなのです。

オンプレミス+クラウドによる ハイブリッドな内部統制対応

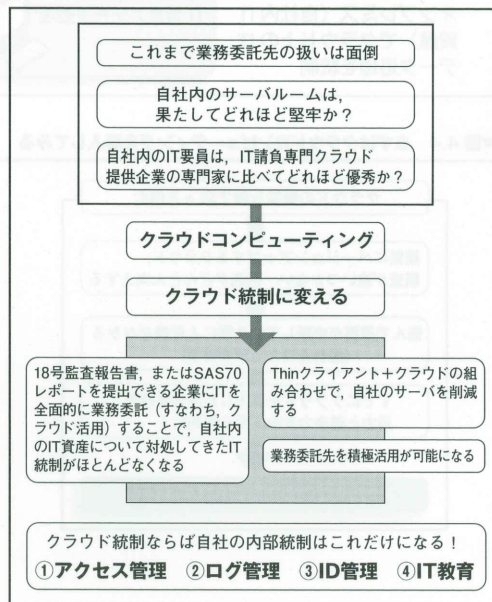


クラウド統制の 3 スタイル

皆さんの企業内では、すでにオンプレミスで既存の IT 資産（ソフトウェアやハードウェアや各種システム）があると思います。なかなか、一気にすべてをクラウドでリプレースできない悩みがあるでしょう。そんなときは、何も一気にすべてをクラウド化しなくても、オンプレミスとクラウドを併用する、筆者が提唱の「ハイブリッド型クラウド」が賢い対応です。

図 4.3 でクラウド統制による IT 統制強化には、3 つのスタイルを示しました。クラウド統制（I）

▼図 4.2 IT 統制から「クラウド統制」への潮流



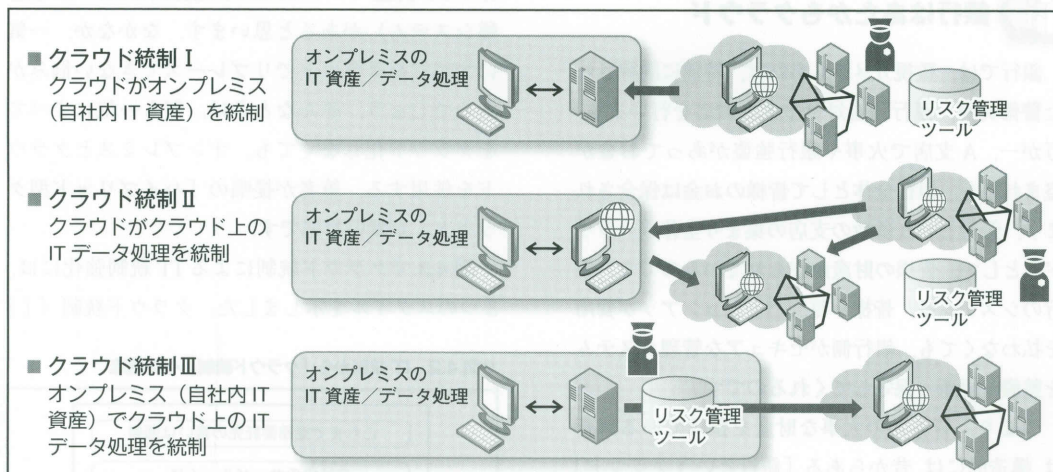
は、既存のオンプレミスのIT環境に、IT統制で監査法人から指摘される対応をする際のリスク管理ツール（例：ログ管理ツール）で、クラウドがオンプレミスを統制する方法です。クラウド統制（Ⅱ）は、すでにクラウドを利用している企業で、クラウド上のデータやシステムを、クラウド上のリスク管理ツールで統制する方法です（クラウドがクラウドを統制）。クラウド統制（Ⅲ）は、クラウド上にあるデータやシステムを、オンプレミスにあるリスク管理ツールで統制する方法です。



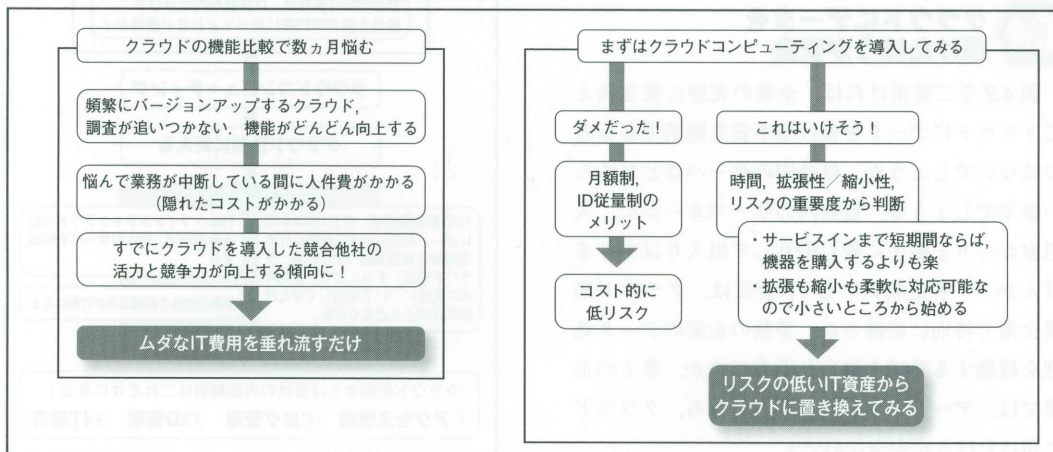
逡巡するよりもやってみては？

どのクラウド統制スタイルを選択するかは、各企業でIT資産の棚卸しをして、どれがクラウド

▼図 4.3 クラウド統制の3スタイル



▼図 4.4 まずはクラウドコンピューティングを導入してみる



活用によって低コスト化／省力化しやすいかを整理して決めれば良いでしょう。また、監査法人の指摘によって、新たなIT統制強化を強いられる際、その指摘をクリアするのにちょうど良いクラウドがあれば、それを利用して低コストで監査対応をすれば良いのです。

また、クラウド活用にあたっては、機能比較を延々と行う方もいらっしゃるようです。図 4.4 にまとめましたが、クラウドの良いところはスモールスタートできるところです。不要なら、投資費用が少ない内にいつでもクラウド活用をやめられます。

従来のITベンダやSIでは、いったん購入したものが最後、ロックインされて使いにくいものを我慢

して使い続けなければならないこともあったでしょう。しかし、クラウドなら、いらないクラウドは即座にやめて、もっと良いクラウドに乗り換えれば良いのです。また、拡張性もさることながら、「そんなに要らないや」と思えば、縮小できるのもクラウドの良さです。

逆に言えば、クラウドベンダにとっては、スイッチングコストが低いため、つねに良いものを提供し続けなければ淘汰されていくことになります。そのゆえ、ユーザ側にとっては、従来のパッケージソフトやシステム構築よりも、ずっと洗練された IT 環境を手に入れやすいと言えるでしょう。

クラウド損益分岐点

素朴な疑問として、「クラウドは万能なのか」という疑問をお持ちの方がいらっしゃるかもしれません。現時点では、基幹システムに関して言えば、クラウドはまだまだ発展途上です。また、クラウド間でのデータ移行ができないケースもあり、クラウドは万能とは言い切れません。

クラウド導入したものの、ID 数での従量制のため、毎年多くの ID 追加費用が従来型のシステムより高くなり、クラウド化をやめて元に戻す企業もありました。あるクラウドが月額定額制か、それとも、ID 数による従量制かなどについて「クラウド損益分岐点」を検討する必要があります。

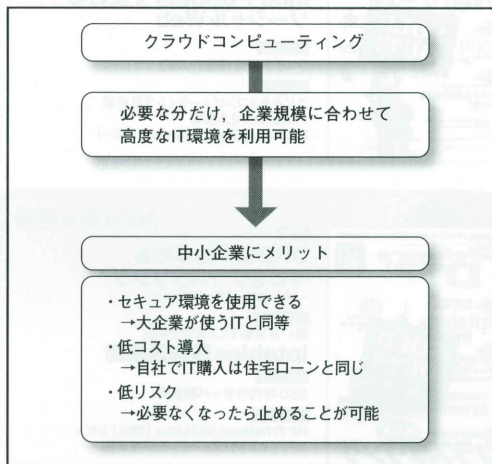
表 4.3 にまとめましたが、クラウド化において、コスト比較シミュレーションをしておくことで良いでしょう。ただし、このコスト算定が曲者で、単にキャッシュとしての投資額以外に、従来型のシステムの保守運用にあたる人件費やダウンタイムの機会損失など、隠れたコスト (Hidden Costs) も管理会計の観点から検討しておく必要があります。

IT 担当者の悩みである保守運用の雑多な処理に、優秀で高給の IT 要員を充てているのは、あまりにもムダです。人件費の固定費化が収益を圧迫してしまいます。また、過酷な労働環境にある IT 要員の方々が、サービス残業で仕事をしていたり、うつ病や労災問題に直面したりするなら、労務リスクが膨張しますし、生産性も下がります。

▼表 4.3 クラウドとオンプレミスの場合の隠れたコストの比較

従来からの問題点	クラウド	オンプレミス
IT を運用するのに必要な隠れたコスト (雑多なメンテナンス対応にかかる人件費)	ベンダ側	IT 要員を教育から始めて、人件費は固定費に追加される
データのバックアップ/リストアにかかるコスト	ベンダ側	自社で二重化、拠点分散、要員の確保

▼図 4.5 IT は大企業のモノからの脱却



この問題をないがしろにする経営は、人をモノとして扱う経営姿勢として望ましくありません。これも、クラウド統制で労務リスクを軽減して解決すべき問題です。

まとめ

図 4.5 に示すように、これまでは資金に余裕のある大手企業だけにしか整備できなかった高度でセキュアな IT 環境を、クラウドのおかげで中堅中小企業や病院・非営利機関でも、安価で身の丈に合わせて導入できるようになりました。

ログの管理を例に挙げれば、ログの分析・収集ツールを従来どおり IT ベンダに依頼すると、初期費用一式で 1,200 万円の見積りでした。クラウドを利用するサービスの場合、同じものを見積ると 75 万円でした。差額は 1,125 万円にもなります。

筆者は、クラウド統制の実践を「IT 奴隷解放宣言」と位置付けています。皆さんが健全なクラウド活用をすることで、競争力が向上がするようになることを祈っております。 **SD**