研究会報告

# 「クラウドコンピューティングのシステム監査（中間報告）」

## －　システム管理基準からのアプローチ　－

2012年　6月　8日

深瀬　　仁（パナソニック溶接システム）

松田　貴典（大阪成蹊大学）

# 研究会のメンバー　（アイウエオ順）

| | 氏名 | 所属（組織） | 参加（団体） |
|---|---|---|---|
| 主査 | 松田　貴典 | 大阪成蹊大学 | JSSA・SAAJ |
| 副主査 | 深瀬　仁 | パナソニック溶接システム株式会社 | JSSA |
| | 足立　憲昭 | | JSSA |
| | 伊地知　裕貴 | 株式会社ニイタカ | JSSA |
| | 浦上 豊蔵 | 三洋ITソリューションズ株式会社　監査グループ | JSSA・SAAJ |
| | 木村　安寿 | 関西学院大学大学院 | JSSA・SAAJ |
| | 雑賀　努 | 株式会社ニイタカ　法務監査室 | JSSA・SAAJ |
| | 佐々木　志津香 | | SAAJ |
| | 城　順平 | イオンリテール株式会社 | JSSA |
| | 高木　実 | | JSSA |
| | 高瀬　宜士 | 帝塚山大学 | JSSA |
| | 飛田　治則 | | JSSA・SAAJ |
| | 野田　正美 | | JSSA |
| | 林　裕正 | 富士通株式会社 | JSSA・SAAJ |
| | 福本　洋一 | 弁護士法人第一法律事務所 | JSSA・SAAJ |
| | 藤井　孝雄 | | JSSA |
| | 森久　　博 | 新日鉄ソリューションズ株式会社金融ソリューション事業本部 | JSSA |
| | 山北　和司 | 株式会社NSソリューションズ関西 | JSSA |
| | 山本　全 | | SAAJ |
| | 吉田　博一 | 大阪府 | JSSA・SAAJ |

# 本日の内容

1. 研究会での活動内容
2. システム管理基準からのアプローチ
3. 今後の活動予定

# 研究会のテーマ

■クラウドコンピューティング（以下、単に「クラウド」と記載する）により、これまでの外部委託形態以上に課題が潜在化し、雲のように実態をつかめない世界になってきている。
本研究プロジェクトでは、クラウドの研究とともに、情報システム活用の問題、情報データの管理や所有の問題、　委託契約問題など、システム監査においてどのような視点やアプローチがあるのか研究を進める。

■当研究会は、
システム監査学会と日本システム監査人協会との
共同プロジェクトである。

■研究会は継続中であり、今回は中間報告である。

# 1．研究会での活動内容

| 会合 | 日程 | 活動内容 | 発表者 |
|---|---|---|---|
| 1回 | 6/23<br>（木） | システム管理基準を用いたアプローチについて<br>進め方の検討 | ― |
| 2回 | 8/5<br>（金） | システム管理基準を用いたアプローチについて<br>整理用フォーマットの検討、チーム編成決定 | ― |
| 3回 | 10/27<br>（木） | システム管理基準を用いたアプローチについて<br>整理用フォーマットの確定、対象会社の想定 | ― |
| 4回 | 12/1<br>（木） | システム管理基準を用いたアプローチについて<br>「情報戦略・企画」での検討 | 各チームの<br>持ち寄り |
| 5回 | 1/12<br>（木） | システム管理基準を用いたアプローチについて<br>「保守」・「運用」・「共通」での検討 | |
| 6回 | 2/16<br>（木） | システム管理基準を用いたアプローチについて<br>「開発」「資産としての考え方」の整理 | |
| 7回 | 3/14<br>（水） | セールスフォースドットコム様から学ぶ | SFDC<br>光田　様 |
| 8回 | 4/19<br>（木） | システム管理基準を用いたアプローチについて<br>・SFDC様の事例から学ぶ　　・読合せ | 各チームの<br>持ち寄り |
| 9回 | 5/12<br>（土） | システム管理基準を用いたアプローチについて<br>全体を通しての読合せと今回の論点整理 | |

# 1．研究会での活動内容　－見えてきた課題－

「企業として導入を決断するのは、難しいのではないか」
という意見が多い

経済的観点だけでなく
クラウド選択の適切性、クラウド管理の整合性を見極める。

クラウドを活用したシステムの品質基準を一定に保証する
マネジメント基準が必要

**システム管理基準をベースに検討をスタート**

# 2. システム管理基準からのアプローチ

## 研究会メンバーにて、「システム管理基準のクラウド版」を作成

システム管理基準のカテゴリに基づき、
5つのチームわけを実施、
「情報戦略・企画」「開発」「運用」「保守」「共通」

| チーム | 参加メンバー　※敬称略 |
|---|---|
| Ⅰ. 情報戦略<br>Ⅱ. 企画 | 木村・雑賀・浦上・飛田 |
| Ⅲ. 開発 | 高瀬・伊地知・山北・佐々木 |
| Ⅳ. 運用業務 | 深瀬・野田・吉田・城・高木 |
| Ⅴ. 保守 | 林・伊地知・藤井 |
| Ⅵ. 共通業務 | 松田・福本・山本・足立・森久・阿部 |

# 2. システム管理基準からのアプローチ

## システム管理基準を変更していくにあたっての視点

元の管理基準との比較を行なえるように整理していく。
- 下段にクラウドにおける管理ポイントを記述
- 下記の項目情報をクラウドにおける特性として付加

| | システム管理(監査)基準と監査のポイント | 確認すべき資料、確認方法 | クラウド区分 | 置換・追加区分 | サービス提供会社へのコントロール内容 | 特記事項 |
|---|---|---|---|---|---|---|
| 現 | 保守業務１．保守手順（１）<br>保守ルール及び保守手順は、保守の責任者が承認すること | | 必要 | 追加 | ・保守契約書を締結しているか<br>・保守手順が書面で明確化されているか | 無し |
| クラウド | **自社のサービスに関係するクラウドシステムの保守ルール及び保守手順をクラウド事業者と開発ベンダー含めた上で合意し、責任者が承認すること。** | クラウド事業における保守手順書 | | | | |

| | |
|---|---|
| **クラウド区分** | クラウドにとって必要か不要かの判断基準 |
| **置換・追加区分** | 管理基準を基とした場合、クラウド用に記入したものが、全くの置換なのか、追記した内容なのかを示す区分 |
| **サービス提供事業者に対するコントロール内容** | クラウドで直接的な管理ができず、間接的な管理としてどのようなコントロールに置き換えるべきかという視点 |
| **特記事項** | 備考欄として活用<br>※特出した想定条件などを明記 |

**「　システム管理基準　－クラウド版－　」　を作成中**

# 2. システム管理基準からのアプローチ

## モデル:システム管理基準を利用する企業・組織の想定範囲

| | |
|---|---|
| **企業規模<br>業種** | 製造業<br>従業員500人、自社内作 有、ｼｽﾃﾑ人員 15名 |
| **ｼｽﾃﾑｲﾒｰｼﾞ** | CRMシステム（顧客管理）<br>低コスト・早期立上げを条件に、1年前に導入 |
| **想定クラウド** | パブリッククラウド（SaaS）<br>※ クラウド事業者以外の開発ベンダーによるアドオン有 |
| **監査ポイント** | **①クラウド選択の適切性（導入前）<br>②クラウド管理の整合性（導入後、管理面）** |

# （参考）クラウドにおけるシステム監査のポイント

※視点はIT内部監査人としてのもの

## （１）クラウド選択の適切性

### ①自社ニーズに対するクラウドの適合性

・クラウドの分類（Public、Privateなど）選択や、クラウドを選択してよい対象なのか？

### ②自社ニーズとSLAの整合性

・稼働率は？（クラウドは意外と高くない）、レスポンスは大丈夫？

### ③オンプレミスとの比較

・オンプレミスと比較して、クラウドのメリットがデメリットを上回っていることを確認

### ④リスクアセスメントの実施

・クラウドにおいて発生しうるリスクに対しての対策　（ex.長時間停止リスク）

## （２）クラウド管理の整合性

### ①監査対象（組織）

・クラウド事業者、自社のクラウド利用部門

### ②監査対象（サービス）と監査範囲

・クラウドの分類と管理責任についての十分な理解

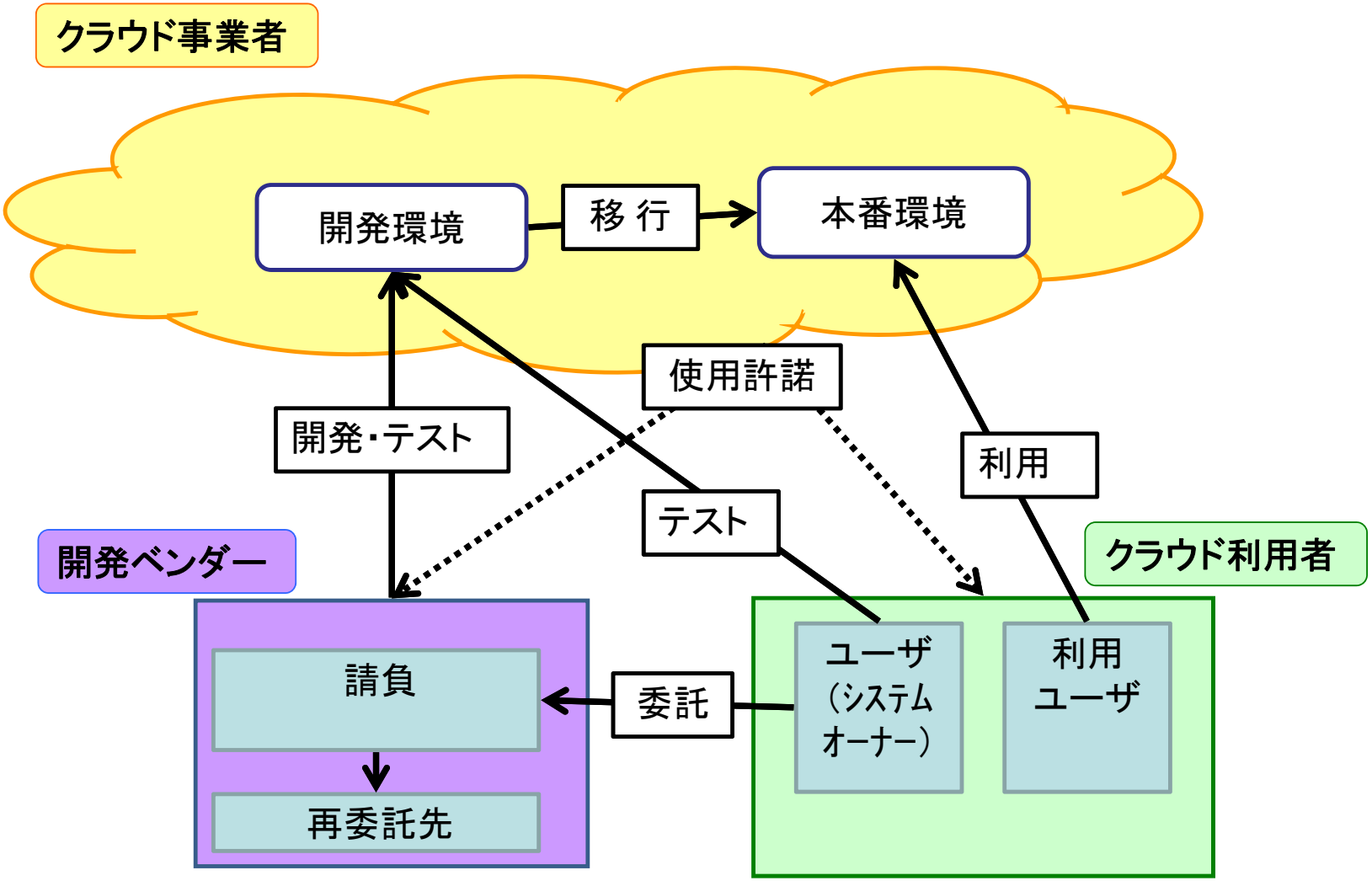
### ③クラウド管理に関する監査の実施

・仮想的ITリソースの管理と物理的ITリソースの管理を分けて考える

（参考：IT内部監査人　生産性出版　ISACA監査基準研究会　著）

# 2. システム管理基準からのアプローチ

## 想定イメージの相関図



# 2. システム管理基準からのアプローチ

**ポイント**

・自社／クラウド事業者／開発ベンダーそれぞれの取組み状況を入手し、自社が求めるレベルを、それぞれの整合性を確保しつつ自社で確認することが重要。
・サービスレベルを担保されていない場合、最悪を想定した復旧しかありえない。
※自社で戦略的にカバーできない業務をクラウド環境で使用できない。

| フェーズ | 論点 | まとめ |
|---|---|---|
| **情報戦略・企画** | 情報戦略・企画フェーズで、クラウドに特化したポイントとしてどこまで論じられるか。 | 経営視点でのクラウド利用に関する決定・承認プロセスが重要。（ｾｷｭﾘﾃｨ・ｺﾝﾌﾟﾗｲｱﾝｽ・BCP対策　等） |
| | 自社が求めるサービスレベルをクラウドで実現できるかどうかの判断を行なえるか。またベンダー能力を適正に評価できるか。 | 関連組織それぞれの内部統制の関連性・整合性が明確であることが重要。<br>実証すること困難⇒見極めルール要 |
| | 資産管理：自社所有の分離、分割が可能か | 資産：利用継続可能かがポイント |
| **開発** | クラウド事業者、開発ベンダー双方から、如何に取組み状況を入手するか。 | 自社ニーズとクラウド事業者、開発ベンダーでの実現イメージの整合性確保。 |
| | マルチテナントによる制約をどう考慮するか | 開発出来ないこと、不向きな点の把握 |
| | 開発期間のみの環境レンタルのケースをどう評価するか。 | 開発環境の利用は委託契約と同様に評価する形でのまとめ。 |

# 2. システム管理基準からのアプローチ

| | 論点 | まとめ |
|---|---|---|
| **運用** | クラウドはあくまでも手段であり、業務委託の観点と類似する。オンプレミスとの境界線、自社で管理不可能なところをサービスレベルや個別契約でどこまで補えるのか。 | クラウド事業者・開発ベンダーから、取組み状況が常に入手可能なこと。<br><br>設計誤りや誤操作によるデータ破壊の修復手段など具体的なリスク対策が関係組織間で検討可能であること。 |
| **保守** | クラウド事業者がｻｰﾋﾞｽﾚﾍﾞﾙを保証するのではなく、実績値公表のみのｹｰｽが多い。自社リスクはどのように考慮すべきか。<br><br>保守の適用範囲はどこまで保証可能か。 | クラウド事業者・開発ベンダーから、取組み状況が常に入手可能なこと。<br><br>クラウドの利用範囲、使い方によって、特性に応じたルールが必要。<br>（移行時の課題、廃棄時の課題など）<br><br>可監査性の保証範囲の見極め必要 |
| **共通** | 自社が求めるサービスレベルをクラウドで実現できるかどうかの判断を行なえるか。<br><br>クラウド事業者・開発ベンダーの能力を適正に評価するための情報を入手できるか。 | クラウド事業者、開発ベンダーの内部統制の有効性が検証できるか（可監査性）<br><br>共通での管理については、まず自社がどうあるべきかを見える化し、そこにクラウドが使えるかの視点が重要。 |

# 3. 今後の活動予定

**今年度は取組み最終年度（研究成果の完成）**

**①システム管理基準　ークラウド版ー　の完成**

**②実用イメージでの最終検証と内容のブラッシュアップ**

成果物

システム管理基準　　ークラウド版ー

# ご清聴ありがとうございました。