研究プロジェクト報告

「クラウドコンピューティングのシステム監査（最終報告）」

― システム管理基準からのアプローチ ―

2013年 6月 7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）

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

研究プロジェクトのメンバー　（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	ﾊﾟﾅｿﾆｯｸ溶接ｼｽﾃﾑ株式会社	JSSA
	伊地知　裕貴	株式会社ニイタカ	JSSA
	浦上 豊蔵	三洋電機株式会社	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	JSSA・SAAJ
	高瀬　宜士	帝塚山大学	JSSA
	飛田　治則	株式会社ルシアン	JSSA・SAAJ
	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
	山本　全	ﾊﾟﾅｿﾆｯｸITｿﾘｭｰｼｮﾝｽﾞ株式会社	SAAJ
	吉田　博一	大阪府	JSSA・SAAJ

©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.

本日の内容

1. 研究プロジェクトでの活動内容（第一期～第三期）

2. システム管理基準の適用
   - アプローチ方法
   - 適用内容

3. 考察
   - 議論になったポイント、今後の課題
   - システム管理基準にて適用できなかった点
   - システム管理基準適用での総括

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

研究プロジェクトのテーマ

■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。

■当研究プロジェクトは、２０１０年５月より開始、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。

■今回の発表は最終報告である。

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

1．研究プロジェクトでの活動内容（2010年度：第一期）

期　間：2010年5月～2011年5月（全7回）
内　容：クラウドを理解し、研究会にて目指す成果物を選定

クラウドの概念整理　（プレ）（第1回）

↓

サービス提供側からの最新動向の研究
- 富士通株式会社　（第2回）
- 株式会社セールスフォース・ドットコム　（第3回）

↓

クラウドに関する法的規制　（第4回）

↓

研究プロジェクトの目指す成果を議論　（第5回）（第6回）

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

1．研究プロジェクトでの活動内容（2011年度：第二期）

期　間：2011年6月～2012年5月（全9回）
内　容：クラウドを対象にしたシステム管理基準の適用研究

進め方の検討（整理用フォーマット、チーム編成）　（第1・2回）

↓

想定対象の絞込みのためのモデル設定　（第3回）

↓

チーム毎に検討内容を持ち寄り議論
（情報戦略/企画業務・開発・運用・保守・共通）　（第4～6回）

↓

サービス提供会社との研究成果の確認　（第7回）

↓

全体を通しての読合せと発表論点のまとめ　（第8・9回）

©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.

1．研究プロジェクトでの活動内容（2012年度：第三期）

期　間：2012年6月～2013年5月（全6回）
内　容：①システム管理基準がクラウドへの適用が困難
　　②クラウドに特化した留意点の考察（最終まとめ）

システム管理基準への適用検討　（第1・2回）

↓

チーム毎の検討結果を再議論
（情報戦略/企画業務・開発・運用・保守・共通）　（第3・4回）

↓

システム管理基準への適用の困難性を討議
クラウド利用への留意点の整理
最終報告資料のまとめ　（第5・6回）

©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.

2. システム管理基準の適用へのアプローチ

**クラウドを活用したシステムの管理水準を一定に保証する
マネジメント基準が必要**

マネジメント基準としてシステム管理基準を採用

「企業として導入を適切に判断するのは極めて難しい」

**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**

©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.

2. システム管理基準の適用へのアプローチ

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 Ⅱ. 企画	雑賀・浦上・飛田・木村
Ⅲ. 開発	伊地知・高瀬
Ⅳ. 運用業務	深瀬・吉田
Ⅴ. 保守	林・伊地知
Ⅵ. 共通業務	福本・山本・松田

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用へのアプローチ

システム管理基準を適用するにあたっての視点

オリジナルの管理基準との比較を行なえるように整理
- 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
現	保守業務1．保守手順（1） 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 ・保守手順が書面で明確化されているか
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を含めた上で合意し、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

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用へのアプローチ

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 業種	製造業 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) 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) ※ 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) ②クラウド管理の整合性(導入後、管理面)**

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用へのアプローチ

クラウドにおけるシステム監査のポイント

（１）クラウド選択の適切性

※視点はIT内部監査人としてのもの

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

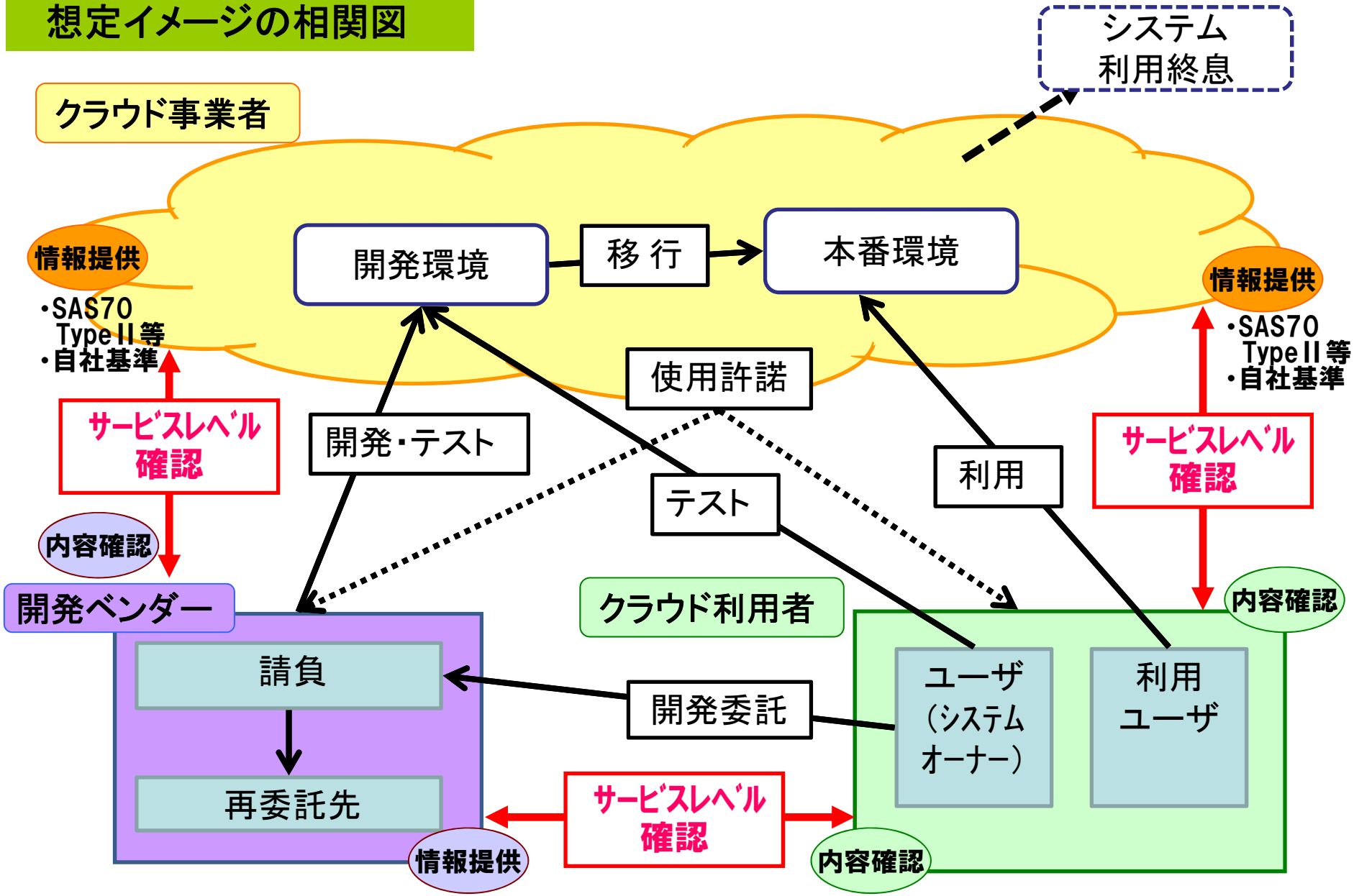
・仮想的ITリソースの管理と物理的ITリソースの管理を分けて考える

（参考：ISACA監査基準研究会 著「IT内部監査人」生産性出版）

©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.

2. システム管理基準の適用へのアプローチ

想定イメージの相関図



©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用　①情報戦略・企画

論点	まとめ
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。（選定基準など） 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。	上流でのリスクの先読みが重要 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・コンプライアンス・BCP・出口戦略　等）

	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	サービス提供会社へのコントロール内容
現	【情報戦略：全体最適化　方針・目標（２）】 情報化投資や情報化構想の決定における原則を定めること。		必要	追加	・クラウド導入事例の入手 ・サービスレベル報告資料の提示と評価
クラウド	クラウドを利用する場合を想定した、情報化投資判断基準を含めていること。				
現	【情報戦略：全体最適化　方針・目標（６）】 情報セキュリティ基本方針を明確にすること。 2）情報セキュリティ基本方針について、組織体の長の承認を受け、企業内外に周知していること。		必要	置換	・情報セキュリティに係るサービスレベル報告資料の提示と評価
クラウド	２）クラウド事業者から情報セキュリティに係るサービスレベルの提出を求め、情報セキュリティ基本方針との整合性を評価して、組織体の長の承認を受け、企業内外に周知していること。	情報セキュリティに係るサービスレベル報告資料と情報セキュリティ基本方針との照合結果 リスク対応計画書、代替案			

©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.

2. システム管理基準の適用 ①情報戦略・企画

	システム管理（監査）基準と監査のポイント（一例）	確認すべき資料、確認方法	クラウド区分	置換追加	サービス提供会社へのコントロール内容
現	【情報戦略：全体最適化 計画の策定（２）】 1）CIO＜以下に共通＞は、全体最適化計画の策定方針において、法令、ガイドライン、基準などコンプライアンス上、考慮すべき外部ルールの遵守、コンプライアンスリスクへの対処、組織体の構成員に対するコンプライアンスの徹底を明文化していること。 4）全体最適化計画の策定時点で法令、ガイドライン、基準などコンプライアンス上、考慮すべき外部ルールをすべて洗い出して、参照可能な状況にしていること。		必要	置換	・クラウド環境のサービスレベルの提示・評価
クラウド	1）CIO＜以下に共通＞は、全体最適化計画の策定方針において、クラウドシステムの稼働環境を想定した国内外の法令、ガイドライン、基準などコンプライアンス上、考慮すべき外部ルールの遵守、コンプライアンスリスクへの対処、組織体の構成員に対するコンプライアンスの徹底を明文化していること。 ※以下 4）～7） も同様に追記。	全体最適化計画 立案にかかる規程 立案ルールの承認記録、立案ルール周知状況			
現	【情報戦略：組織体制 情報システム部門（２）】 情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門家、権限付与、外部委託等を考慮した体制にすること。		必要	追加	・サービス対象範囲の提示・評価
クラウド	クラウドシステムの導入に伴い、情報システム要員を業務部門内に配置するなど、情報システム部門が業務側に近づき実務知識の習得と業務ニーズの収集をより積極的に行える体制を構築できること。	人員配置計画			

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用 ①情報戦略・企画

	システム管理（監査）基準と監査のポイント（一例）	確認すべき資料、確認方法	クラウド区分	置換追加	サービス提供会社へのコントロール内容
現	【企画業務：開発計画（１）】 開発計画は、組織体の長が承認すること。		必要	追加	・契約時期（更新時期）の明示と評価
クラウド	・クラウドの契約時期（更新時期）を明示すること。 ・テスト系と本番系を持つ場合、その契約内容を明示すること。 ・関係者にリスク管理責任者、法務責任者を加えること。	契約書			
現	【企画業務：開発計画（３）】 開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。		必要	追加	・サービス対象範囲の提示・評価
クラウド	・開発物の所有先について明示すること。 ・クラウド使用の妥当性、業者選択の妥当性を検証すること。 ・クラウドを用いない場合との比較を行なうこと。 ・システムデータを監査、税務上のエビデンスにしている場合は契約完了時の対応を明らかにすること。 （法務担当者の了解を得る。）	開発計画書			

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用 ②開発

論点	まとめ
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。 マルチテナントによる制約をどう考慮するか。 開発期間のみの環境レンタルをどう評価するか。	利用者ニーズとクラウド事業者、開発ベンダー それぞれの実現イメージの整合性確保が重要。 開発出来ないこと、不向きな点の把握。 開発環境の利用は委託契約と同様に評価。

	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	サービス提供会社への コントロール内容
現	【開発業務：開発手順（１）】 開発手順は、開発の責任者が承認すること。		必要	追加	・開発・テスト環境の提供方法の提示・評価 ・開発リソース情報の提供と評価
クラウド	クラウド事業者が提供する開発・テスト環境の確認。 （性能評価、セキュリティ、移行策、開発環境の保持要否） 環境特有の開発リソース（言語・ツール）の活用要否を利用責任者が判断すること。	サービスレベル確認書 環境特有の開発リソース活用時の評価表 （メリット・デメリット）			
現	【開発業務：開発手順（３）】 開発手順は、開発の規模、システム特性等を考慮して決定すること。		必要	追加	・SaaSアプリのリリース計画 ・標準／オプション／要開発の情報提供と評価
クラウド	SaaSアプリのリリース計画を考慮して、決定すること。 開発できないこと、不向きな点を把握すること。	SaaSアプリリリース計画 開発リソース：開発標準			
現	【開発業務：開発手順（４）】 開発時のリスクを評価し、必要な対応策を講じること。		必要	置換	・クラウド環境の想定リスク一覧の提示と評価
クラウド	クラウド特有の想定リスクを加え、評価し、必要な対策を講じること。 （クラウド環境のバージョンアップへの追随確認など）	クラウド特有のリスク表			

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用 ③運用

論点	まとめ
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ﾋﾞｽﾚﾍﾞﾙや個別契約でどう補うか。	クラウド事業者・開発ベンダーから、取組状況を常に入手。ｻｰﾋﾞｽﾚﾍﾞﾙどおり運用されているか、常にﾓﾆﾀﾘﾝｸﾞできる仕組みが存在していること。

	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	ｻｰﾋﾞｽ提供会社へのコントロール内容
現	【運用：運用管理（10）】 事故及び障害の影響度に応じた報告体制及び対応手順を明確にすること。		必要	追加	・障害時運用ルール、仕組みの提示
クラウド	クラウド事業者からのエスカレーション方法がｻｰﾋﾞｽﾚﾍﾞﾙ確認書に明記され、利用責任者がその内容を承認していること。	ｻｰﾋﾞｽﾚﾍﾞﾙ確認書 障害連絡網			
現	【運用：運用管理（11）】 事故及び障害の内容を記録し、情報システムの運用責任者に報告すること。		必要	追加	・障害発生時の対応履歴の提示
クラウド	事故および障害は、適時にユーザ部門に伝達される仕組みがあり、事故・障害発生時には、クラウド事業者がｻｰﾋﾞｽﾚﾍﾞﾙどおり運用していることを検証すること。	ｻｰﾋﾞｽﾚﾍﾞﾙ確認書 障害時運用ルール 障害対応履歴			
現	【運用：運用管理（12）】 事故及び障害の原因を究明し、再発防止の措置を講じること。		必要	追加	・再発防止策の提示方法
クラウド	ｻｰﾋﾞｽﾚﾍﾞﾙ確認書に基づきクラウド事業者から再発防止策が伝達され、その実効性を確認していること。	ｻｰﾋﾞｽﾚﾍﾞﾙ確認書 再発防止策			

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用 ③運用

論点	まとめ
クラウドシステムを導入することにより、情報システム部門の役割が、単なるシステムの開発、運用から変化する。システム要員の極端なスリム化ではなく活用を考慮する必要がある。	クラウドシステムにより、運用負荷が軽減されるため、情報システム要員はよりユーザ支援を行う業務に配置するなど、情報システム部門の役割と人員配置を再考する必要がある。

	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	サービス提供会社へのコントロール内容
現	【運用：運用管理（１３）】 情報システムのユーザに対する支援体制を確立すること。		必要	追加	・クラウド対象業務範囲の明確化
クラウド	既存システムのクラウド化に伴い、運用業務の実態がクラウド事業者に移転することを鑑み、要員再配置によるユーザ支援体制の確立を考慮すること。	サービスレベル確認書 ユーザ支援体制表 人員配置計画			
現	【運用：運用管理（１５）】 情報システムの稼動に関するモニタリング体制を確立すること。		必要	追加	・稼動実績の入手
クラウド	サービスレベル確認書に基づきクラウド事業者が保証する稼働率が満たされていることを定期的にモニタリングする体制を確立すること。	サービスレベル確認書 クラウド稼動実績			

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用 ④保守

論点	まとめ
クラウド事業者はｻｰﾋﾞｽﾚﾍﾞﾙを保証するのでなく、実績値公表のみのｹｰｽが多い。 利用者の自社リスクはどのように考慮すべきか。 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、取組状況が常に入手可能なこと。 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。（ 移行時・廃棄時の課題 ） 可監査性の保証範囲の見極め必要

	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	ｸﾗｳﾄﾞ区分	置換追加	ｻｰﾋﾞｽ提供会社へのコントロール内容
現	【保守：保守手順（１）】 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	・保守契約の締結可否 ・保守手順書の提示と評価
クラウド	利用者は、サービスに関係するクラウドの保守ルール及び保守手順をクラウド事業者と開発ﾍﾞﾝﾀﾞｰそれぞれの間で合意し、利用責任者が承認すること。	ｻｰﾋﾞｽﾚﾍﾞﾙ確認書 クラウド事業における保守手順書 保守対象内容一覧			
現	【保守：保守手順（３）】 保守時のリスクを評価し、必要な対応策を講じること。		必要	追加	・クラウド事業者の保守体制は明確か。 ・保守担当者のスキルは十分か。 ・保守体制は確立されているか。
クラウド	クラウド事業者が行う保守作業のリスクを、クラウド事業者を含めて評価し、対策を講じること。	ｻｰﾋﾞｽﾚﾍﾞﾙ確認書 ｸﾗｳﾄﾞ保守実績			

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用 ④保守

	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	ｸﾗｳﾄﾞ区分	置換追加	ｻｰﾋﾞｽ提供会社へのコントロール内容
現	【保守：保守の確認（１）】 変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。		必要	追加	・保守契約の締結可否 ・保守手順書の提示と評価
クラウド	変更したアドオンプログラムのテストの実施は、保守のテスト計画に基づいて、開発ﾍﾞﾝﾀﾞｰと利用者システム部門にて共同で実施すること。その際、クラウド事業者の問合せ先も明記しておくこと。	ｻｰﾋﾞｽﾚﾍﾞﾙ確認書 クラウド事業における保守手順書 保守対象内容一覧			
現	【保守：保守の確認（２）】 変更したプログラムは、影響範囲を考慮し、テストを行うこと。		必要	追加	
クラウド	変更したプログラムの影響範囲の調査は、開発ﾍﾞﾝﾀﾞｰが、クラウド事業者への調査を十分に行い、その結果を利用者にて検証すること。	ｻｰﾋﾞｽﾚﾍﾞﾙ確認書 変更内容確認表			

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

2. システム管理基準の適用　⑤共通

論点	まとめ
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。 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） まず利用者がどうあるべきかを見える化し、そこにクラウドが適用できるかの視点が重要。

	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	サービス提供会社へのコントロール内容
現	【共通：品質管理　計画（１）】 品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。		必要	追加	・委託契約書の内容提示と評価
クラウド	クラウド事業者との契約内容に関わる品質管理の計画は、クラウド事業者との委託契約の締結権限者も承認すること。	サービスレベル確認書 委託契約書・約款			
現	【共通：委託・受託　計画（１）】 委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。		必要	置換	・開発ベンダーの選定基準の提示と内容評価
クラウド	通常、クラウド事業者とはクラウド使用（使用許諾）、開発ベンダーとは業務（アプリケーション）開発委託関係が発生。クラウド事業者の選定は、クラウドの特性を評価し、適用する業務の対象範囲を見極める。さらに、活用するクラウド事業者の選定と共に、そのクラウド事業者の提携する（推薦する）開発ベンダーの選定を最適化計画の中に盛り込むことが重要となる。	使用許諾契約書 委託契約書 開発ベンダー選定基準			

©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.

2. システム管理基準の適用　⑤共通

	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	サービス提供会社へのコントロール内容
現	【共通：災害対策　リスク分析（１）】 地震等のリスク及び情報システムに与える影響範囲を明確にすること。	リスク分析マニュアル リスク棚卸し表 リスク評価書	必要	置換	・リスク分析マニュアル、サービスレベル確認書の内容提示と評価
クラウド	クラウド事業者からクラウドに用いるリソースに対する地震などのリスク及び情報システムに与える影響範囲の特定に必要な情報提供を受けそれらを明確にすること。	リスク分析マニュアル リスク棚卸し表 リスク評価書 サービスレベル確認書			
現	【共通：災害対策　リスク分析（２）】 情報システムの停止等により組織体が被る損失を分析すること。	障害影響分析表	必要	置換	・障害影響分析表と、サービスレベル確認書の内容提示と評価
クラウド	クラウド事業者からリスクや影響範囲の情報を得て、システム停止等により組織体が被る損失を分析すること。 ・クラウド事業者から情報システムの停止及び機能縮退がどのような状況下で、どのような範囲で発生するのか、発生頻度も含めて情報提供を受け、その結果、自社業務にどのような影響を及ぼすことになるのか、充分に分析を行なうこと。	サービスレベル確認書 障害影響分析表			
現	【共通：災害対策　リスク分析（３）】 業務の回復許容時間及び回復優先順位を定めること。	業務別許容回復時間表 リスク分析書・評価書	必要	置換	・リスク分析書・評価書、サービスレベル確認書の内容提示と評価
クラウド	クラウド事業者の復旧手順を前提に、回復許容時間や優先順位を定めること。組織体の方針に合わない場合クラウドの適用を止めることも判断すること。	サービスレベル確認書 業務別許容回復時間表 リスク分析書・評価書			

©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.

3. 考察：議論になったポイント、今後の課題

・クラウド導入の場合、
情報戦略・企画フェーズでのリスクの先読みが重要

※CIOの役割に変化をもたらす

短期間で経営・IT両視点で自社のリスクを把握し
クラウド導入・継続を判断できるスキル

・『所有』⇒『使用』に伴ない、
自社の情報システム現場での運用業務が減少

自社の情報システム要員は、よりユーザ支援を行う業務
（ﾌﾟﾛｾｽ・ﾃﾞｰﾀ分析等）への配置比率が高まるため、
人員計画・教育への反映が必要

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

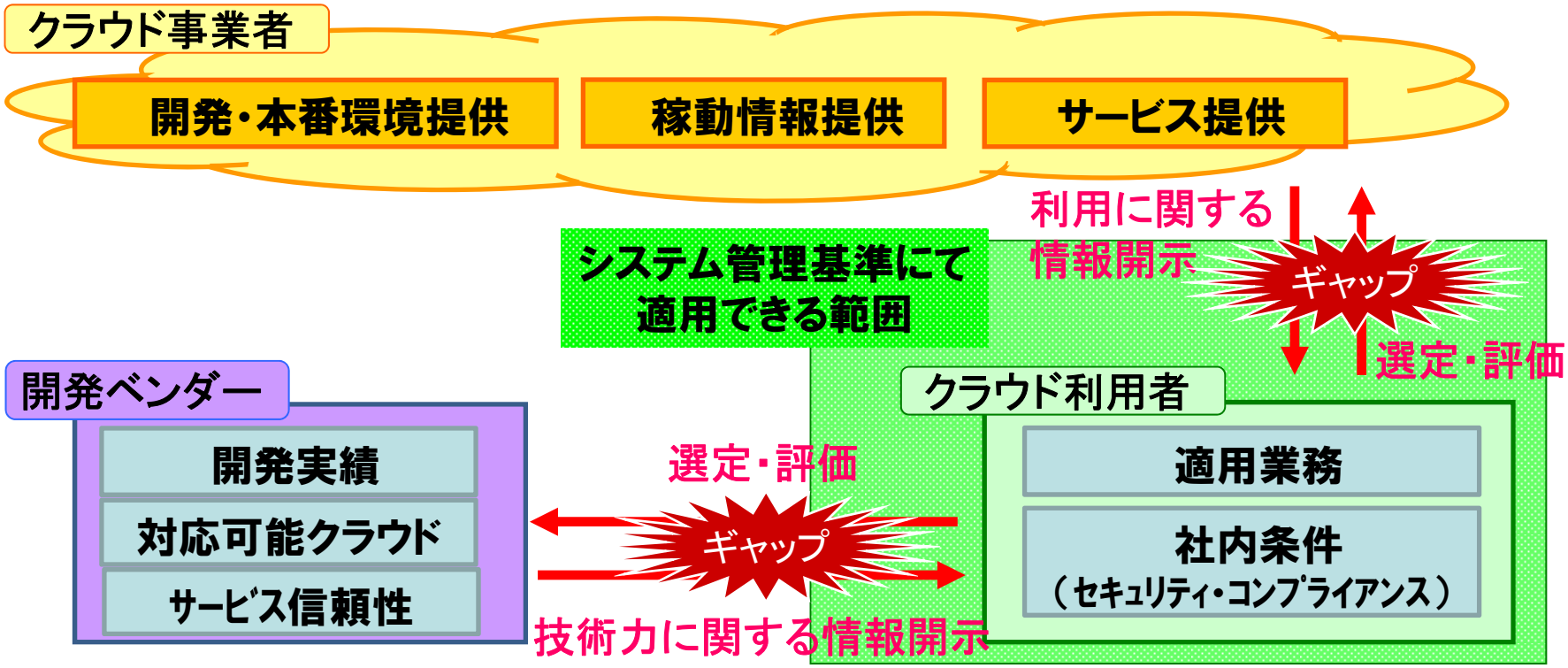
3. 考察:システム管理基準にて適用できなかった点

利用者が所有しない仕組みのシステム管理基準への適用は困難

クラウドサービスの選定、継続利用、契約期間、終了にあたり、経営層が合理的な判断をするための評価指標が必要

しかし【システム管理基準】は、利用者が自社で管理できるもの（責任）を自社でいかに管理し評価しているかがポイント。（網掛け部分）

クラウド事業者は、あくまでもサービスを提供しており、サービス責任は、契約・約款内容に留まる。（結果、限定的な監査しか実現できない。）



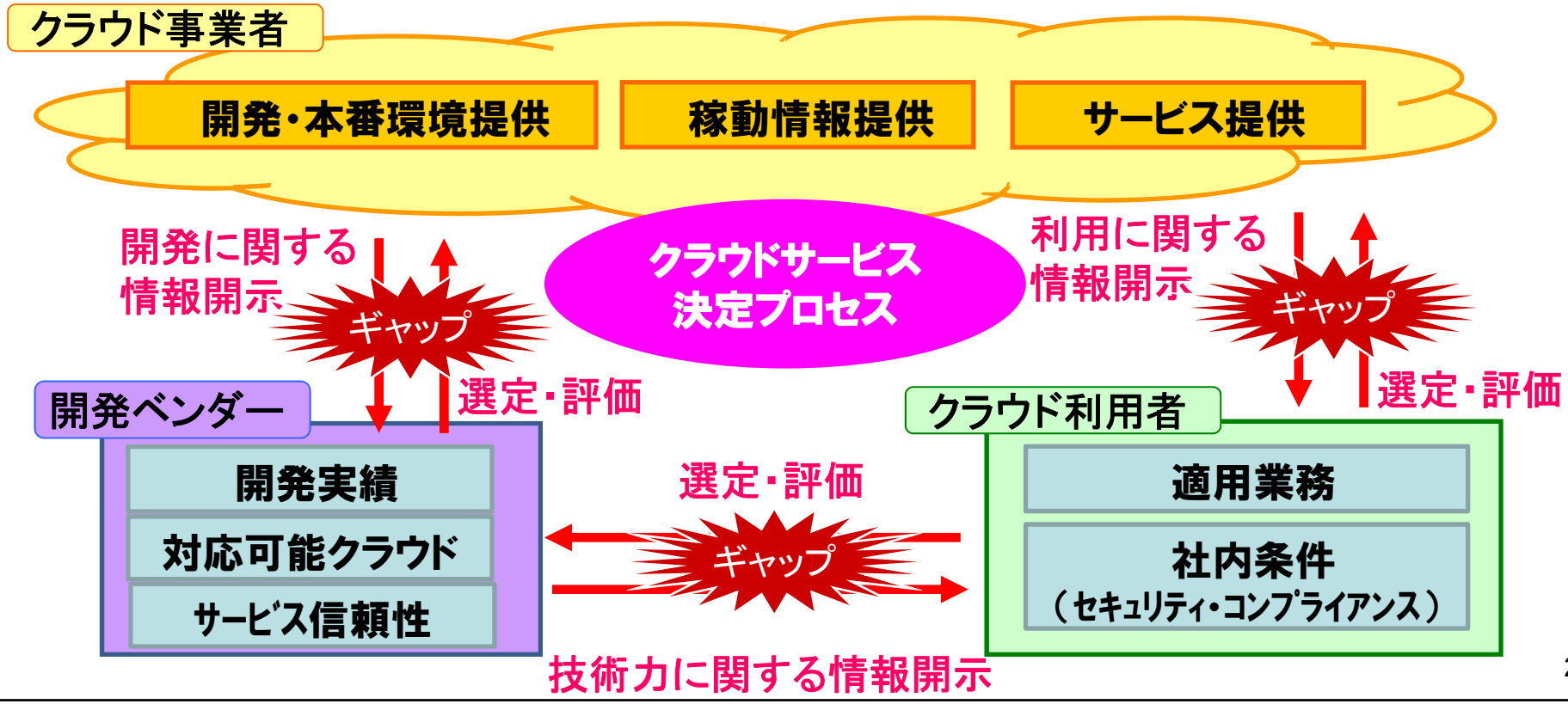
©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.

3. 考察:システム管理基準適用での総括

クラウド利用者、クラウド事業者、開発ベンダーそれぞれの間で発生する
ギャップを埋めるために必要なことをルール化する。

クラウドサービス決定プロセス

- クラウド利用者が求める「選定基準」「選定レベル」 のルール化
- 複数のクラウド事業者を同様基準で比較・選定するため、
  クラウド事業者からの「情報開示内容」 のルール化(利用時・開発時)



©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

3. 考察:システム管理基準適用での総括

研究会開始当初と比べ、クラウドに求められる内容が大きく変化

（例）

●対象業務範囲
- 今までシステム化しにくかった領域(周辺) ⇒ 基幹系システムへの活用開始

●導入障壁
- すぐ止められる ⇒ 一旦導入するとなかなか止められないシステムへの拡大

●情報の安全性の考え方
- 他社の導入状況や安定性が確認できてから ⇒ まずはクラウドでやってみる

クラウドが今後、より重要なシステムに活用され始めた場合、データの流出や消失など、重大事故発生リスクをあらかじめ想定しておくことが大事

クラウドに特化した選定基準は必要
（クラウドサービス決定プロセスの策定）

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

ご清聴ありがとうございました。

©2013 JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」 All right reserved.

©2013　JSSAシステム監査学会-「クラウドコンピューティングのシステム監査研究プロジェクト」　All right reserved.