＜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成果報告＞

「クラウドコンピューティングのシステム監査（中間報告）」

"System auditing of cloud computing (interim report)"

2011年6月10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）	JSSA
	阿部　政夫	伊藤忠テクノソリューションズ株式会社	JSSA
	伊地知　裕貴	株式会社ニイタカ	JSSA
	浦上 豊蔵	三洋ITソリューションズ（株）　監査グループ	JSSA・SAAJ
	加藤　篤	愛知県信用保証協会	JSSA・SAAJ
	亀田　裕和	情報技術開発株式会社　監査室	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
	酒井　哲夫	追手門学院大学、コムチュア（株）、情報技術開発（株）	JSSA
	城　順平	イオンリテール（株）	JSSA
	高木　実		JSSA
	高瀬　宜士	帝塚山大学	JSSA
	田崎　竹雄		SAAJ
	津田　　博	近畿大学　経営学部	JSSA・SAAJ
	飛田　治則		JSSA・SAAJ
	林　裕正	富士通株式会社	SAAJ
	福徳　泰司		JSSA
	福本　洋一	弁護士法人第一法律事務所	JSSA・SAAJ
	森久　　博	新日鉄ソリューションズ(株)金融ソリューション事業本部	JSSA
	安尾　勝彦	(株)オオコシ セキュリティコンサルタンツ	JSSA
	山北　和司	株式会社NSソリューションズ関西	JSSA
	吉田　博一	大阪府	JSSA・SAAJ

目　次

1．研究会のテーマと今回の発表要旨

■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、システム監査人協会との共同プロジェクトである。

■今回は中間報告である。

2. 活動実績　①活動履歴

全7回実施(継続中)

会合	日程	活動内容	発表者
プレ	5/14（金）	クラウドコンピューティングについて	岡谷 亨　氏
1回	7/16（金）	クラウドコンピューティングの概観と システム監査面から見た課題	森久　博　氏
2回	8/27（金）	クラウドコンピューティングへの富士通の取組み	若林　毅　氏
3回	10/14（木）	Salesforceのセキュリティ対策/システム監査ご紹介–	内田　仁史　氏
4回	12/10（木）	「クラウドの利用に対する法的規制について」	福本　洋一　氏
5回	2/3（木）	「中間のまとめ:今後の進め方について」	深瀬　仁
6回	5/18（水）	「研究会:中間報告資料のレビュー」	深瀬　仁

2. 活動実績　②2010年度の取り組み内容

クラウドの概念を学ぶ　（プレ）（第1回）

↓

サービス提供側からの最新動向のご紹介

- 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）

↓

クラウド利用に関する法的規制　（第4回）

↓

研究会の目指す成果を議論　（第5回）（第6回）

3. クラウドの定義 ①NISTの場合

自由に設定可能な共有のコンピュータ資源(ネットワーク・サーバ・ストレージ・アプリケーションサービスなど)の集積に対する利便性の高い、オンデマンドのアクセスを可能とするモデルであって、最小限の管理努力やサービス提供者とのやりとりで迅速な提供や回収が可能なもの。(NIST:2009.10.07より)

クラウドの特性として、NISTでは以下の5点が挙げられている。

On-demand self-service	オンデマンドセルフサービス
Broad network access	広範なネットワークアクセス
Resource pooling	地理的制約がないリソース共有
Rapid elasticity	利用に応じた拡張・縮小性
Measured Service	サービス性能の測定可能

3. クラウドの定義　②クラウドの特徴を整理

分類	メリット	デメリット（課題）
オンデマンド セルフサービス	・利用者視点で要求に応じたサービスの享受	・求めるサービスレベルと提供されるサービスレベルに差が発生
広範なネットワークアクセス	・一般のネットワークを経由し、アプリケーションを「所有」せず「利用」	・一般回線を経由するため、ネット上の脆弱性対策が困難（フィッシング、マルウェア対策） ・多様な装置（スマートフォンなど）からのセキュリティ対策が急務
地理的制約がないリソース共有	・マルチテナント実現によるトータルコストダウン ・災害対策、負荷分散に対応	・データ保管場所の特定は困難 ・保管場所が海外だと日本の法律を適用できず、また消去確認も困難 ※監査対応に不向き
利用に応じた拡張・縮小性	・規模に応じてすぐ実現 ・ピーク時のみの拡張も可 ・一時的なシステムには最適	・利用者が増えるとID単価の積上げでオンプレミスより高価になる可能性有 ・ベンダーロックイン（他社切替困難）
サービス性能の測定可能	・リソースの使用状況をコントロールし最適化	・サービス性能はあくまでSLA範囲内での保証 ・障害時に利用者側にて対応不可

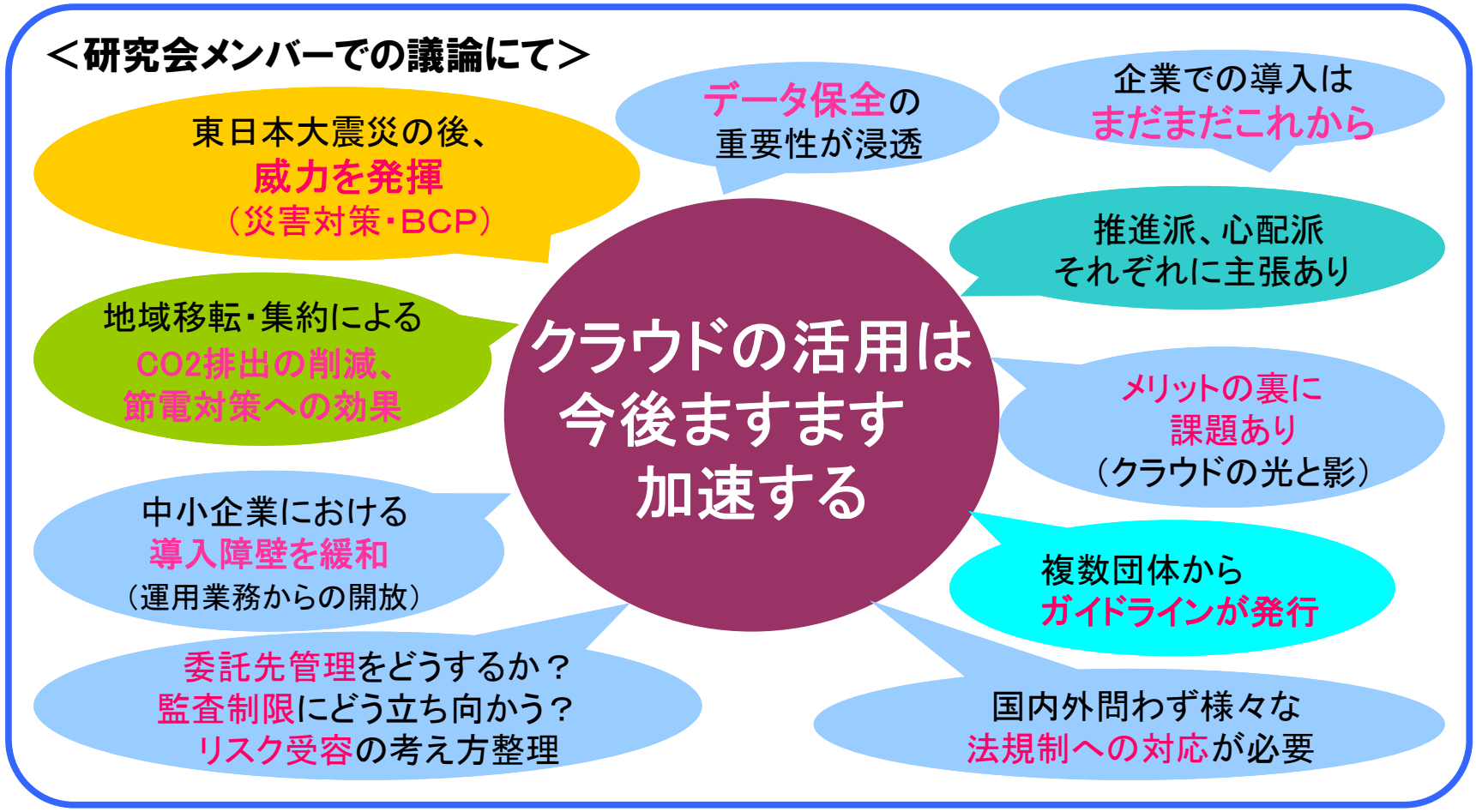
3. クラウドの定義　③クラウドの分類

分類	内容
Public Cloud	不特定多数の人々や大規模な業界団体などに提供され、 クラウド･サービスを販売する組織により所有される。
Community Cloud	コミュニティ向けのシェアードサービスとして提供される。
Private Cloud	特定の利用者を対象とし、専用のITリソースをもとに提供される。
Hybrid Cloud	上記複数のクラウド分類から、2つ以上を組合せて提供される。

分類	内容
SaaS	ネットワークを経由してアプリケーションを利用
PaaS	顧客が開発したアプリケーションをクラウドで提供 （そのためのプラットフォームを提供）
IaaS	サーバ（処理能力）、ストレージ、ネットワークなどを 借りるサービス

3. クラウドの定義 ④当研究会において

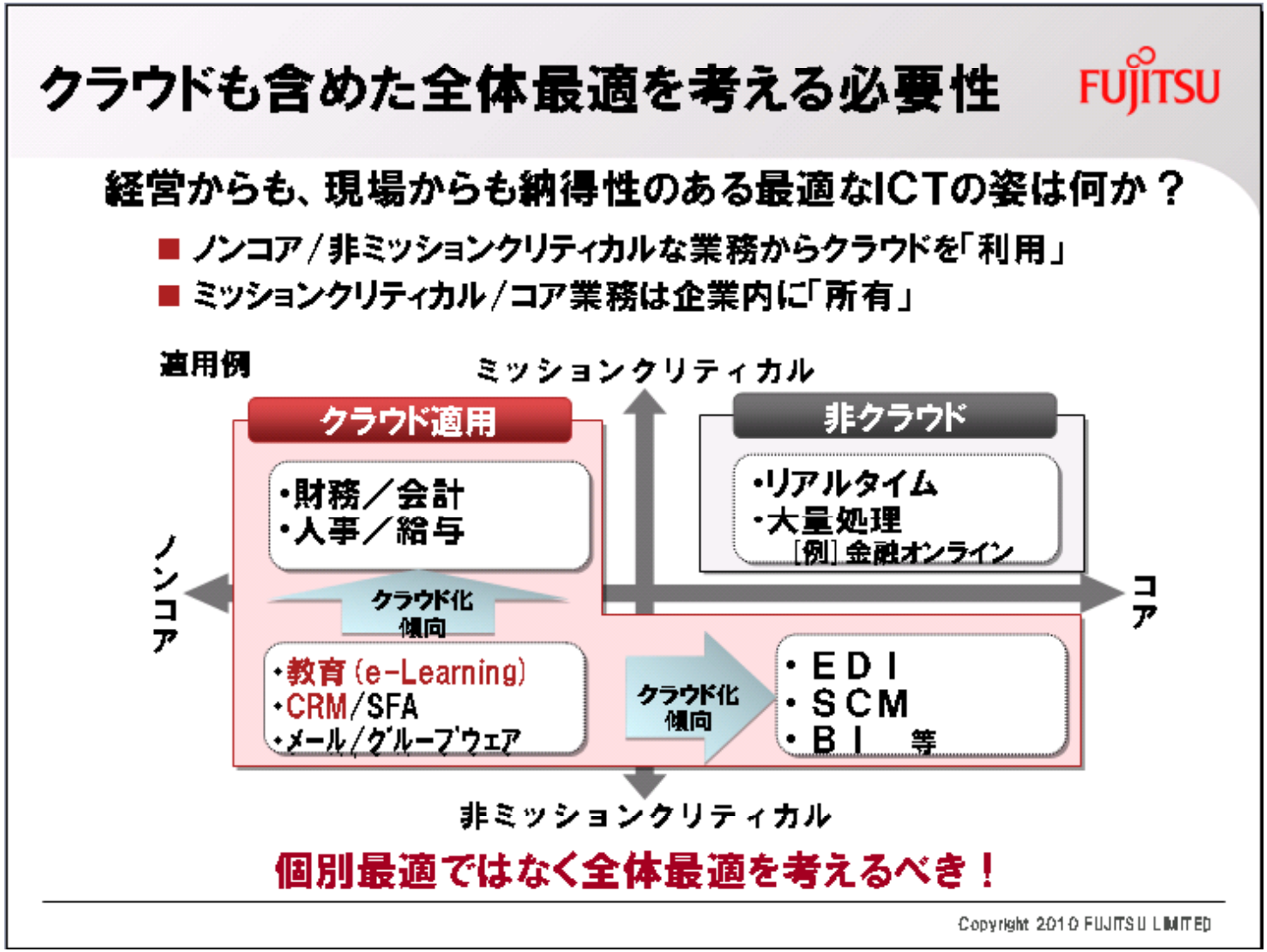
利用者、サービス提供者、それぞれにて様々な解釈が存在



※最終報告時には、研究会としてクラウドの定義を整理する。

4. サービス提供者側の取組み ～富士通の場合～

クラウドに特化するのではなく、全体最適の視点でICTの姿を企画立案

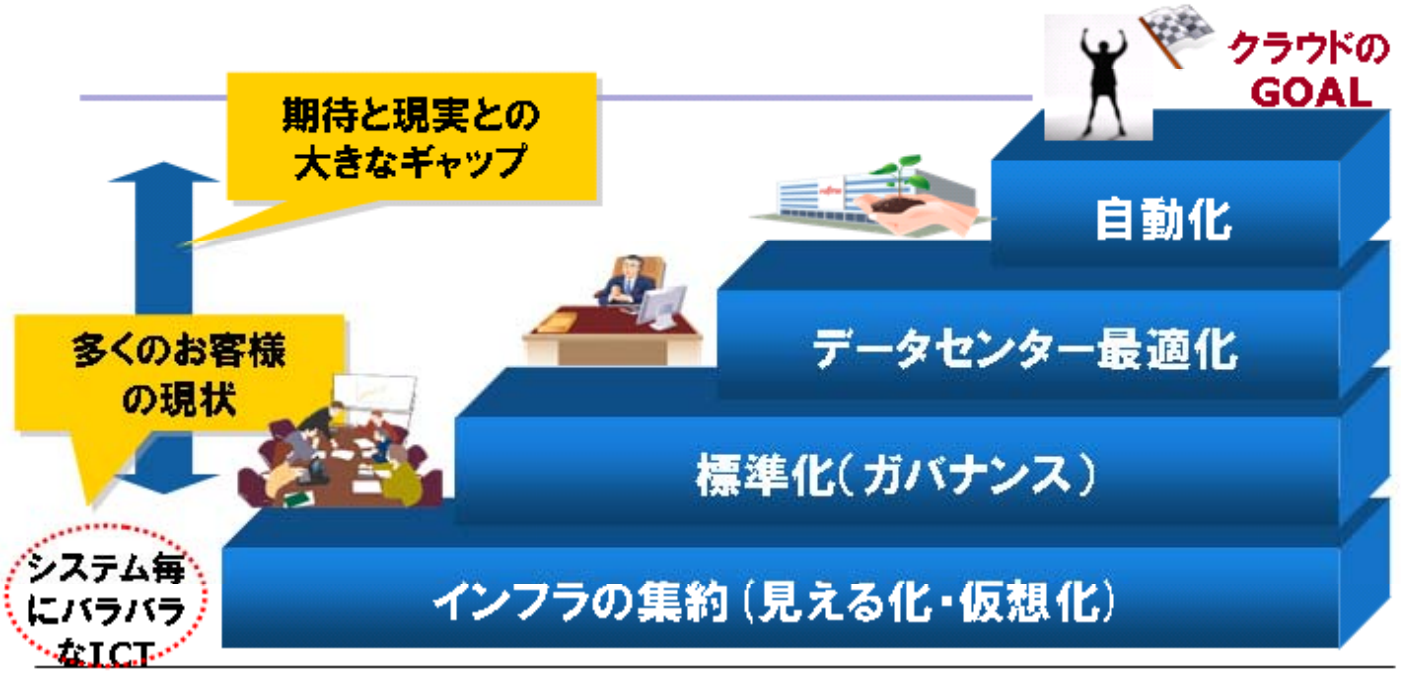


4. サービス提供者側の取組み ～富士通の場合～

標準化(ITガバナンス)が進まないとクラウド化の真のメリットを享受できない。

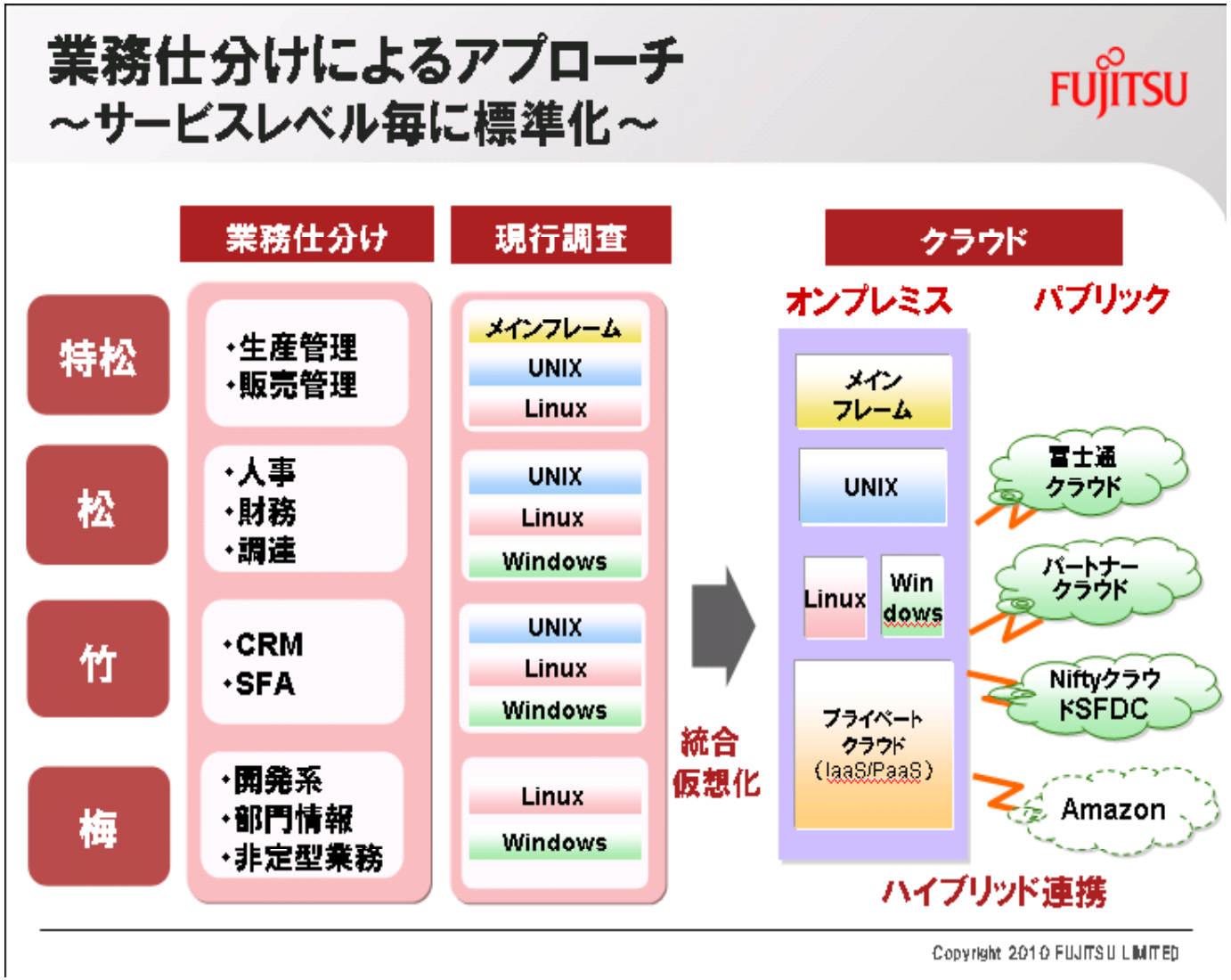
クラウド検討で気付くITガバナンスの重要性 FUJITSU

■ インフラのクラウド化には、情報システム部門の利用ユーザに対するサービスレベル定義やセキュリティポリシーなどのITガバナンスが前提
■ クラウド化の真のメリットを享受するためには、標準化のハードルを越える必要性



4. サービス提供者側の取組み ～富士通の場合～

業務仕分けによるアプローチを実施



4. サービス提供者側の取組み ～富士通の場合～

サービスレベル毎にパターンを共通尺度として定義

運用の業界標準のITILをベースにインフラ設計に関連する項目を抽出
全ての組合せを検討するのではなく、“ありえるパターン”を既存のシステムとの対比で検討

①サービスレベル（要素）

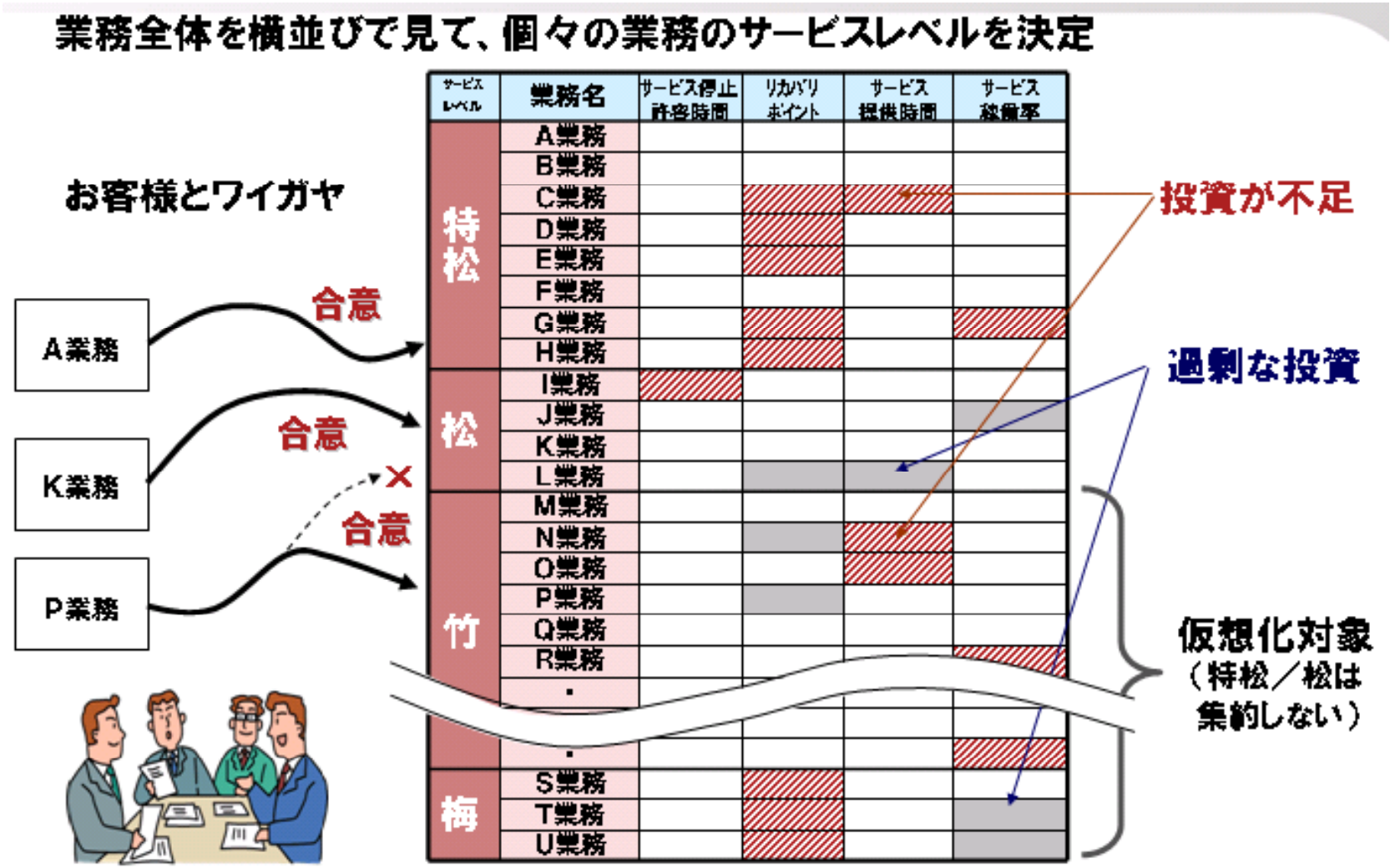
分類	レベル要素	レベル 5	4	3	2	1	0
可用性	(a) サービス停止許容時間	無停止	10分以内	1時間以内	4時間以内（半日）	8時間以内（1日）	ベストエフォート
維持性	(b) データリカバリポイント	データ更新の直前	直近のバックアップ 当日複数回更新	直近のバックアップ 定期（日次）			
維持性	(c) サービス提供時間	365日 24H	365日 8:00～24:00	365日 8:00～20:00			

②サービスレベルパターン（共通尺度）

サービスレベルパターン SLA要件	特松（最高）	松（高）	竹（中）	梅（低）	その他（最低）
サービス停止許容時間	4	3	2	1	1
データリカバリポイント	5	5	3	2	0
サービス提供時間	5	4	2	1	0

4. サービス提供者側の取組み ～富士通の場合～

業務仕分けによるアプローチを実施し、サービスレベル毎に標準化



4. サービス提供者側の取組み ～富士通の場合～

運用の標準パターンを策定し、サービスレベル毎の実施状況を可視化

運用の標準パターン化

FUJITSU

■ クラウド化の検討を進めると、運用の標準化
■ 運用・保守作業体系に基づき、運用標準パターンを策定

作業区分1／サービスメニュー	作業区分2／サービス項目	特松	松	竹	梅
TK010 運用・保守実施管理	TK0 0010 運用・保守実施管理	●	●		
TK020 事業継続計画	TK020010 事業継続計画の維持管理				
TK030 外部監査	TK030010 外部監査対応				
UK010 サービスレベル管理	UK0 0010 サービスレベル設定	●			
	UK0 0020 サービスレベル測定	●			
	UK0 0030 サービスレベル分析・評価	●			
UK020 サービスデスク	UK020010 Q&Aトラブルの受付け・回答	●	●	●	
	UK020020 定型要求の受付け	●	●	●	
	UK020030 要望・クレームの受付け	●	●	●	
	UK020040 利用者への通報・アナウンス				
	UK020050 ナレッジ管理				
UK030 インシデント管理	UK030010 インシデント発行管理	●	●	●	●
	UK030020 インシデント対応状況管理	●	●	●	●
	UK030030 インシデント分析・評価	●	●	●	●
	UK030040 重大障害発生時の復旧統制	●	●	●	●
UK040 問題管理	UK040010 問題発行管理	●	●		
	UK040020 問題対応状況管理	●	●		
	UK040030 問題分析・評価	●	●		

4. サービス提供者側の取組み ～富士通の場合～

利用者プロセスから課題と確認すべき事項を整理 ⇒ SLAの締結

■ 利用者プロセスからの課題整理と確認すべき事項

フェーズ	課題例	利用者自身が確認すること
戦略・方針フェーズ	・クラウド委託業務の経営的判断 ・クラウド事業者の選定	・契約約款及びSLAの内容、信頼性の確認 ・事業者の**サービスロードマップ**の確認 ・事業継続性の確認
準備フェーズ	・利用者が要求するレベルの実現の可否	・サービスレベル（稼働率、可用性（冗長化）、提供機能） ・**セキュリティレベル**（アカウント管理方法、認証方式、暗号と鍵管理） ・アプリケーション、データの**ポータビリティ**性（API、移行ツール） ・**モニタリング機能**（対象と内容） ・ログ機能（対象と内容、取得方法）と監査内容の確認
開発・導入フェーズ	・ベンダー**ロックイン**の回避	・各種ライセンスの確認 ・事業者間の相互運用性の確認 ・アプリケーション、データの移行ツールの検証
運用フェーズ	・契約遵守状況の確認方法	・**各種ログ**（利用者認証、アクセス、オペレーション、リソース消費）の確認 ・法令順守状況の確認 ・**監査報告書**の確認
利用変更フェーズ	・途中変更でのペナルティ ・事業継続の不備 ・別事業者への移行ができない	・利用変更後のデータ、アプリケーション移行ツールの確認 ・利用変更に伴うデータの消去状況
利用終了フェーズ	・データやアプリの適切な消去	・契約終了に伴う、**データの消去**（DoDのデータ消去基準） ・利用終了者のアクセス権の削除
コンプライアンス各種制度	・個人情報保護法	・クラウド事業者の**個人情報**の的確な管理の確認と監督
	・不正競争防止法	・営業機密情報の**秘密管理要件**の確認
	・成果物の著作権	・利用者作成のデータやプログラムの**著作権**の確認
	・会社法、金融商品取引法（内部統制）	・クラウド事業者に預けた情報の適切な収集と確認（取締役会）
	・カントリリスク	・海外の場合データセンターの**準拠法**の確認

※SLA: Service Level Agreement
※DoD: United States Department of Defense（アメリカ合衆国国防総省）

4. サービス提供者側の取組み ～富士通の場合～

（参考）

■ クラウド・サービスレベルのチェック項目の一例

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例
◆アプリケーション運用					
1	可用性	サービス時間	サービスを提供する時間帯(設備やネットワーク等の点検,保守のための計画停止時間の記述を含む)	時間帯	24時間365日 (計画停止/定期保守を除く)
2		サービス稼働率	サービスを利用できる確率((計画サービス時間－停止時間)÷計画サービス時間)	稼働率(%)	99.9%以上(基幹業務) 99%以上(基幹業務以外)
3		重大障害時の代替手段	早期復旧が不可能な場合の代替措置	有無	バックアップデータの取得が可能なホームページを用意
4	信頼性	システム監視基準	システム監視基準(監視内容/監視・通知基準)の設定に基づく監視	有無	ハードウェア/ネットワーク/パフォーマンス監視
5		障害通知プロセス	障害発生時の連絡プロセス(通知先/方法/経路)	有無	指定された緊急連絡先にメール/電話で連絡し、併せてホームページで通知
6		ログの取得	利用者に提供可能なログの種類(アクセスログ、操作ログ、エラーログ等)	有無	セキュリティ(不正アクセス)ログ/バックアップ取得結果ログを利用者の要望に応じて提供
7	性能	オンライン応答時間	オンライン処理の応答時間	時間(秒)	データセンタ内の平均応答時間3秒以内
8	拡張性	カスタマイズ性	カスタマイズ(変更)が可能な事項/範囲/仕様等の条件とカスタマイズに必要な情報	有無	利用画面上の項目配置変更や新規項目の追加が画面より設定可能
9		外部接続性	既存システムや他のクラウド・サービス等の外部のシステムとの接続仕様(API※、開発言語等)	有無	API(プログラム機能を外部から利用するための手続き)を公開
◆サポート					
10	サービス提供時間帯(障害対応)		障害対応時の問合せ受付業務を実施する時間帯	時間帯	24時間365日(電話)
11	バックアップの方法		バックアップ内容(回数、復旧方法)、データ保管場所/形式、利用者のデータへのアクセス権、利用者に所有権のあるデータの取扱方法など	有無/内容	日次で差分バックアップ、週次でフルバックアップを取る。遠隔地にテープ形式保管。アクセス権はシステム管理者のみに制限など

4. サービス提供者側の取組み　セールスフォース・ドットコムの場合

OECDの3大基本概念（C. I. A）に基づき、大規模なセキュリティ投資を実施、更に監査性の考え方を加えて、総合的な情報セキュリティ対策を実施

管理項目	対応内容
機密性 Confidentiality	・大規模投資による世界最高水準のセキュアシステム ・限定された管理者による集中管理 ・職務分掌と相互検証体制 ・お客様のみが情報にアクセス可能 ・サードパーティによる脆弱性チェック ・グローバルオフィスでISO27001認証取得
保全性 Integrity	・センター内データスナップショット ・世界規模のデータセンター間リアルタイムレプリケーション ・日次テープバックアップ ・お客様サイトへのバックアップオプション
可用性 Availability	・冗長化（N+1）システム ・フライホイール発電による電力バックアップ ・99．9%以上の稼働率実績 ・平均300ms以下のページ処理時間
監査性 Auditability	・Trustサイトで稼働状況を公開 ・総務省「ASP・SaaS安全・信頼性に係る情報開示認定」に基づく情報開示 ・SAS70 TypeⅡ　監査レポートを年二回提供可能

4. サービス提供者側の取組み　セールスフォース・ドットコムの場合

「規模の経済」による大規模な情報セキュリティ投資が可能
- 1社で対応するには限界があるセキュリティ投資

マルチテナントによる効率性を実現
- 1つのコード、1つのシステムとして全体を管理 （シンプル）

厳格なデータアクセスコントロール
- 管理者は「データ」にアクセスできるが「情報」にはアクセス不可
- データベースにアクセスできるのは米国本社の少数の人間のみ

企業内のロングテールアプリケーションへ高度なセキュリティを実現
- 今までコストを多くかけられなかった部門システムなどにも適用可能

稼働状況の公開と認定制度や外部監査機関の活用
- trust.salesforce.com による情報公開
- 「ASP・SaaS安全・信頼に係る情報開示認定制度」
- 「SAS70TypeⅡ」監査完了（半年ごとに報告書作成）

4. サービス提供者側の説明から見えてきた課題

・マルチテナントによる監査制限が発生
⇒ユーザ企業からの直接監査は事実上困難

・SAS70（TypeⅡ）、第18号監査だけでは不充分

利用部門にて、リスク分析を行ない、
事前見極め・採否評価プロセスが重要

クラウドを採用する際、自社規約に
どう反映すべきか。反映できるのか。
（リスク受容を書面に残せるか）

経営者が株主から訴追されないために
なすべきことはなにか。

今後の検討材料

5. クラウド利用に関する法的規制について

■クラウドの多様性から、クラウドに共通する法的リスクの整理が困難
■ユーザ企業はクラウド事業者の所有または管理するIT資源に対して十分なコントロールを及ぼすことができない場合が多い。

対象情報（例）	法的規制	クラウド利用のポイント
①個人情報	個人情報保護法 ・安全管理措置（20条） ・委託先の監督（22条）	ユーザ企業は情報の委託先であるクラウド事業者に対し情報管理について監督義務を負う。 ⇒ 安全管理措置を遵守させるための契約の締結等が必要
②営業秘密	不正競争防止法 ・秘密管理性指針	営業秘密としての法的保護を受けるには秘密管理性の要件を満たす必要 ⇒ アクセス制限・秘密としての認識可能性等の機能がクラウド事業者によって提供されることが必要
③第三者の著作物	著作権 ・複製権（21条） ・公衆送信権（23条） ・間接侵害　など	第三者の著作物についてはライセンサーから許諾された範囲内でのみ複製等が可能 ⇒ 第三者であるクラウド事業者の所有・管理するサーバへの複製等がライセンサーから許諾されていることが必要

5. クラウド利用に関する法的規制について

対象情報（例）	法的規制	クラウド利用のポイント
④電磁的記録	e-文書法 電子帳簿保存法	・見読性（情報を即座に読み取れる）、 ・完全性（改竄、消失などの防止） ・機密性（第三者による不正アクセスや情報・漏えい等の防止） 検索性（必要な情報を効率的に選別可能） ⇒ これらの要件を満たす機能がクラウド事業者から提供されることが必要
⑤技術情報	外国為替及び外国貿易法	暗号化技術情報等については輸出について国の許可を得る必要がある ⇒海外サーバを利用するクラウドで情報を管理する場合は許可を得ることが必要
⑥海外サーバ内の情報	EUデータ指令 愛国者法（USA) データ規制操作権限法(中国）	国内法ではなくサーバが所在する国の法律の適用を受けるおそれがある ⇒ 情報が管理されているサーバの所在地を限定・確認できることが必要

6. 当研究会の今後の方向性

①サービスを利用する側の取り組み

- ガイドライン作成／サービス採用までの経緯
- 定期棚卸、契約更新時の見極め方法　など

②監査制限に対しての対抗策の検討

③想定事例をもとにしたケーススタディの実施

ご清聴ありがとうございました。