Salesforce Industry Paper

外部委託のリスク管理とクラウド

～金融業界における外部委託に係るリスク管理の世界動向とクラウド利用～

概要

2016 年 7 月、シンガポールの金融監督当局である MAS（Monetary Authority of Singapore）が新しい外部委託管理のガイドラインをリリースした。これを機に、世界の当局の外部委託に対するスタンスをまとめてみた。なぜ外部委託なのか。それは、世界各国の金融監督当局は共通して、クラウドは外部委託の一形態とするという認識だからだ。外部委託に係る規制やガイドラインを知ることは、金融監督当局のクラウドに関するスタンスをまとめることにほかならない。以下に、認識されるリスクと、必要なリスク管理の方策、そしてセールスフォース・ドットコムの対応をまとめる。

エグゼクティブサマリー

- 現在の世界各国の金融当局の IT におけるフォーカスエリアは①サイバーセキュリティ②テクノロジー（Fintech も含む）③外部委託である。世界の主たる当局では、「外部委託に係るリスク管理の重要性」は無視できない大きなテーマとなっており、新しい規制やガイドラインが次々に発行されている。
- 外部委託先による障害や、情報漏洩などの重要なインシデントがそのきっかけである。
- 外部委託に対する各国の規制の強化やガイドラインの制定は、金融機関にある懸念を生んだ。それは、規制当局が業務の外部委託、とりわけクラウドの利活用に消極的なのではないかというものだ。
- 各国の規制やガイドラインで求めていることは、適正なリスク管理とガバナンスであり、決してクラウドの利活用に制限をかけるものではない。
- MAS で 2016 年 7 月 27 日に外部委託先管理のガイドラインが新しく発行された。ここでは、金融業界におけるクラウドの幕開けとも言える画期的な内容が盛り込まれていた。というのは、厳格な規制で金融機関を監督し、畏怖の対象であると思われていた監督当局が、クラウドの健全な利用を積極的に指南したからである。
- セールスフォース・ドットコムのクラウド基盤は、これらのガイドラインにも沿うものである。金融機関をはじめとする各インダストリーでのクラウド利活用について、事業者側のリスク管理になんら懸案すべき事項はなく、むしろ積極的な ICT 利活用の最適な解であると言える。

目次

はじめに

外部委託は1960年頃からリストラクチャリングの一環として行われてきた。しかし、時を経ると「コスト削減」や「人員削減」などの目的から、「より質の高い効果的なサービスを顧客に提供するリエンジニアリングの手段」として考えられるようになった。最近では顧客ニーズの多様化やビジネスのスピード化への対応、ビジネス構造の柔軟性確保、経営資源の効率的活用といったさまざまな目的と局面で外部委託が行われている。リスク管理の観点から捉えると、従来自社内で抱えていたシステムや業務リスクは委託先に移り、構造も変化せざるを得ない。これらに対処するには、委託する業務に応じたリスク管理体制を自社内に整備し、適切に運用していくことが重要となる。

本稿では、特にこうした動きが顕著な金融業界の動向や事例を中心にまとめた。世界各国で調査やヒアリングを展開し、ITの外部委託全般に係るリスク、特に外部委託の一形態であるクラウドコンピューティングの利活用に関するリスク管理を考察。そのうえで、クラウドファーストを安心して実現するには何が必要か、セールスフォース・ドットコムが提供できることについても言及している。これらの内容はすべての業界に共通した課題であり、その管理や対応も共通することを付け加えておきたい。

1．外部委託を取り巻く環境

2006年、2012年、2014年に、国内の地域金融機関では、外部委託先の作業者によるカード偽造事件が発生、その都度、リスク管理のあり方が注目されてきた。海外でも2012年に発生した英銀行大手「ロイヤル・バンク・オブ・スコットランド(以下「RBS」)」のシステム障害は、外部委託先の問題として大きく取り上げられた。また米国でも最近、委託先ベンダーがハッキングされ個人情報が漏洩していたにもかかわらず、金融機関が長期間その事実を把握していなかった事例があった。これらの事件を契機に、各国の金融監督当局では一斉に、外部委託先管理の規制強化が活発化した。このことは社会インフラである金融機関で顕在化したが、業界を問わずリスクへの対応が求められている。シンガポールでも2010年のDBS銀行のシステム障害(委託先の復旧手順の誤りにより全面ダウン)、2013年のStandard Chartered における外部委託先システムへのハッキングによるデータ流出が発生。事件をきっかけに外部委託管理に対する問題意識が高まり、規制強化の動きにつながっている。

2. 市場動向

金融業界のIT外部委託の市場は、景気の後退期と回復期においてその構造がやや異なる。景気後退期ではコスト削減を期待して外部委託が増加するが、景気回復期では規模の大きい金融機関は内製化に舵を切り、従来の大手ベンダーへの大規模委託は減少する。他方、中小金融機関ではインドのベンダーなど、中小規模かつ高度に専門化された高付加価値なサービスへ委託を増やす傾向にある。「コスト削減」から「差別化のための業務委託」へシフトしているのだ。中小の金融機関では、人材の枯渇といった課題が背景にあるとも言えるがそれだけではない。既存のシステムに縛られる部分が少なく、大規模な変革に外部委託を利用するなど戦略的な判断をしやすいことも理由の一つであろう。

コスト削減を目的とした海外外部委託「オフショアリング」はどうであろうか？ 外部委託の面で有効手段には違いないが、データ保護に関連する各国の規制や法律の影響を考えると一概に積極的とは言えない。文化や言語の違い、頻繁な人材の入れ替わりに絡んだ退職時の情報不正持ち出しなど、セキュリティやプライバシー保護を懸念する声は否定できない。特に個人情報を含むトランザクションに係る運用を委託する場合では、オフショアリングの活用は難しいと考える金融機関や企業は多い(全面的に禁止されているわけではないが、上記セキュリティやプライバシー保護に対する懸念事項に加え、「関連する法制度をすべて把握し、リスクを事前に認識して対応するのは困難」というのが共通認識であろう)。

近年、オフショアではリスク管理を十分にできない場合に、「ニアショアリング」の利用が増加している。これは、統治が及びやすい国内、しかも労働力が安い地域のベンダーに委託をし、コスト削減と統治のしやすさのメリットを得るソリューションである。

特に米国においては、政府(立法、雇用確保)や経済(従来のオフショア先の賃金高騰)のプレッシャーに加え、高離職率、低生産性、知識やノウハウの外部流出、もしくは言語的な問題を解決する目的で、ニアショアリングの活用が増えている。Citibankが米国向けのデータセンターをフロリダに構築したケースはその典型だ。

以上、一般的なITの外部委託について、その市場動向について述べてきたが、クラウドコンピューティングについても同じ市場傾向にあると言える。

そもそも金融業界では、各国の金融監督当局の共通認識としてクラウドコンピューティングは外部委託の一形態として整理される。事業者によっては「資源共有型のクラウドコンピューティングは、サービスをそのまま利用するモデルであり、外部委託とは性質を異にする」との主張もある。しかし金融業界では、特に重要なデータを扱う場合もしくは重要なシステムをクラウドで実現する際、クラウド事業者に統制の効かない状況でサービスを利用することはありえない。日本における金融庁にかぎらず、各国の当局も利用者側の金融機関に対し、利用するサービスの提供事業者への厳格なリスク管理と説明責任を求めているのである。

クラウドコンピューティングに求められるものも、従来のコスト削減という基軸から、新しい機能の採用による競合他社との差別化や、そのアジリティによる迅速な早期市場導入など、戦略的な価値を求める方向に変わりつつある。

中小や新興金融機関を始め多くの企業は、競争力の獲得・維持のために新規サービスをいち早く市場に投入しようとする意識が強い。そのため、自社開発よりも専業ベンダーへの外部委託（専業クラウドサービスの利活用）により、スピードを上げることはもはや自然の流れと言える。このことはモバイルやソーシャル、クラウドといった先進的テクノロジーの台頭によって確実となった。

3．諸外国の外部委託（クラウド）に関連する規制・ガイドライン

外部委託では、「リスク管理」や「法令遵守」などの機能が、規制対象となっていない第三者へ移転する可能性がある。そのため、当局の監督下にある企業が規制上の義務をいかに果たすかが課題となる。当局の頭の痛いところでもあり、結果こうした課題に対処するため、外部委託を行うには企業に相応のリスク管理を求めざるを得ない。

各国の金融監督当局は規制やガイドラインを準備している。従来のガイドラインに付加的なペーパーを都度発行していくケースや、近年の急激な環境変化に対応する形で全面的に発行し直すなど運用はさまざまだ。その意図は概ね上述の通りであり、クラウドの利活用に関するガイドラインもこの外部委託のリスク管理に包括されているケースがほとんどである。日本の金融業界では、「公益財団法人金融情報システムセンター (以下「FISC」)」で、一昨年度開催された「金融機関におけるクラウド利用に関する有識者検討会」を受けてクラウド関連の安全対策基準を充実させた。しかし、世界においてクラウド固有のガイドラインを準備しているケースは稀である。以下に 主要各国の外部委託、またはクラウドに関する規制・ガイドラインをまとめた。

主要各国金融当局の発行するクラウドに関する法規制、ガイドラインの例

金融当局	時期	文書名	概要
オーストラリア APRA	2010/11	“OUTSOURCING AND OFFSHORING Specific considerations when using cloud computing services”	・ビジネスの継続性、機密性、完全性、他の法律や規制遵守、適切なリスク管理 ・クラウド固有の規制はない –アウトソーシング（APS231,GPS231,PPG231） –ビジネス継続性（APS232,GPS222,LPS232, AGN232,GGN222,PPG233） –IT セキュリティリスク管理（PPG234）
シンガポール MAS	2011/7 2013/6 2014/9 **2016/7**	“INFORMATION TECHNOLOGY OUTSOURCING”通達 TRMG(Technology Risk Management Guideline) チェックリスト準備 Consultation Paper: NOTICE ON OUTSOURCING GUIDELINE ON OUTSOURCING **Guideline on Outsourcing Risk Management**	・完全性、回復性、機密性、法準拠、監査性契約終了時の資産のデータ消去 ・外部委託によってビジネスの継続性が損なわれないこと ・金融機関がデータの物理的保管場所を把握し、データに他のデータが混入したり、他人がアクセスするリスクを完全排除し、必要に応じて安全に消去できること etc ・クラウドも明確に Outsourcing の Guideline の対象として明示、2004 年の Outsourcing Guideline の改訂 1. MAS との関わり（事前報告） 2. リスク管理（リスク評価、事業者評価、契約、機密性とセキュリティ、BCP、モニタリング、監査と検査、国外への外部委託、系列会社への委託、内部監査のアウトソーシング）
フィリピン BSP	2013/8	“Monetary Board approves the enhanced Information Technology Risk Management Framework for BSP–Supervised Institution”	・ITRM Framework の拡張とクラウドへの適用
オランダ DNB	2012/1	“Circulaire Cloud Computing” 通達	・リスクを明確に認識し、軽減措置を図ること ・第三者へのアウトソーシングが当局の監督を妨げないこと
	2012/5	“Cloud computing: the risks and how they are supervised”	・アウトソーシングと同じ要件でカバーされるべき ・データアクセス権者及び物理的格納場所に関する契約が必要 ・当局の監査権の確保
	2012/11	“DNB removes hurdle towards “outsourcing the cloud”	・マイクロソフトが DNB の求める監査権と当局検査受忍義務を契約条項に入れることに同意 （対象 Office365） ・他国の金融規制監督当局とも連携し、クラウド事業者に対して同様の契約条項を盛り込むように働きかけ 2013/1 Salesforce.com 2013/7 アマゾンウェブサービス（AWS） とも同様の合意
米国 FFIEC	2012/7	“ Outsourced Cloud Computing”	・2011/12 に NIST の発行した“Guidelines on Security and Privacy in Public Cloud Computing” に追従 ・Cloud Computing が Outsourcing の一形態と明示 但し、クラウド特有のリスクも考えるべき 1. デューデリジェンス ・データ分類と必要に応じたデータ保全策（暗号化） ・データの分離 ・リカバリー性（クラウド事業者の業務継続）

			2. ベンダー管理 3. 監査 4. 情報セキュリティ 　データの区分とアクセス管理 　データ保護 　セキュリティの脅威や事故対応の効果的なモニタリング 5. 法規制、風評被害 6. クラウド事業者とネットワーク事業者が適正な計画とリソースを持っているか
米国 FDIC	2012/5	“Managing Emerging Technology Risk”	・リスク管理、ベンダー管理、IT セキュリティポリシーの更新 ・クラウド環境に出るデータの明確化（データ分類） ・データ分類が金融機関のポリシーに従って行われること ・バーチャルマシン環境におけるハイパーバイザーやバーチャルマシンマネジャーに対する適切な管理 ・データ暗号化（クラウド事業者内伝送、伝送路、クラウド事業者内蓄積データ） ・SaaS の場合、定期的なデータバックアップのコピーを委託元金融機関が読めるようなフォーマットで（事業者側でのバックアップは読めないフォーマットかも） ・BCP（クラウドサービスのコンティンジェンシープラン） ・契約終了時の戦略、復帰計画
カナダ OSFI	2012/2	“New technology-based outsourcing arrangements” （こうした通達を出すことは極めて異例）	・Guideline B-10“Outsourcing of Business Activities, Functions and Processes”（2009 年 3 月）は現在も有効。これに準拠するように繰り返しクラウドコンピューティングは新規テクノロジーベースのアウトソーシングサービスの一部 1. 機密性、セキュリティ、資産分離 2. コンティンジェンシープラン 3. レコードの所在 4. 監査権 5. 再委託 6. 重要業務についてのモニタリング
ベルギー NBB	2012/10	“Attentes prudentielles en matière de Cloud computing”	・クラウドはアウトソーシングの一形態 ・アウトソーシングのガイドラインに準じる ・規制を守る限り、当局の事前承諾は不要ではあるが、ガバナンス実施状況に関して事前の情報提供が必要
英国 UK FCA,PRA		Handbook “Senior Management Arrangements, Systems and Controls” SYSC8	・アウトソーシングの EU の金融商品市場指令(MiFID)ではクラウドの利用可否については明言なし。ICO（The Information Commissioner’s Office）のスタンスを懸念(データ保管場所の特定ができない)している節がある ・クラウドはアウトソーシングそのもの ・上記 Handbook で論点カバー可能 　①技術面　②契約時のデューデリジェンス　③パーソナルデータ保護　特に③については金融機関がリスクを理解していない（特に再委託、再々委託が絡む場合） ・FCA 経由でクラウドに関して何かしらのペーパーを出す

			予定は今のところない（2015 年時点） ・クラウド導入に際して事前許可は不要。ただしコア業務については事前説明を求めている ・監督当局の検査権、委託元金融機関の監査権（全てのデータセンター存在場所に対する物理的アクセス） ・金融機関の内部監査機能を活用し、結果をレビューするという運用が伝統的 ・G 社は検査、監査の受忍を拒否している為、クリティカル業務へのサービス提供は認めない
EC EBA（欧州銀行監督機構）		当面なし	・当機関のガイドラインは組織・体制・リスク認識や管理プロセスなどに関する原則を記載。技術的事項はBSI(British Standards Institution)等の標準化団体のガイドラインに任せる（クラウドの扱い） ・クラウドは外部委託の一類型（データを金融機関から外に出す）外部委託と同様の項目で管理が必要。以下は考慮必要 ①データセンター(データ格納場所）特定が難しく、かつEU 域外のケースもあり ②関与する事業者の数が把握しにくく、外部委託と比較して透明性が低い ・クラウドに特定した基準の策定の計画はない（BSI も同様） ・機密性、可能性の維持は重要で、当局の検査や FI の監査権の確保は必須 ・監査受入を拒否するサービスは利用すべきではない ・ISO 認証や SOC2 等の第三者監査結果の代用についてはこれでカバーできない項目について別の代替的な手法での評価が必要（外部委託の扱い） ・金融機関のコア業務は外部委託すべきではない ・金融機関による統制、監査の実施が必要 ・必要な IT の可用性、安全性を委託業務についても充足 ・委託のシステムを戻すこと（内製化）が可能 ・EU はパーソナルデータ保護の要請が厳しい->暗号化対策や VPN の確保といった技術的視点も重要 （同一金融グループ内の海外拠点への持ち出しには寛容） ・小規模な金融機関は基準充足の為に業態別団体が共同化の受け皿に。こうした業態別団体は各国当局のモニタリングの対象になっている

表のように、各国では、金融機関におけるクラウドコンピューティングの利活用に対する規制、ガイドラインなどが出されている。これらは皆、外部委託時の大規模障害を契機とし、健全な金融業務運営に必要なリスク管理を明確にすることが目的だ。決して外部委託もしくはクラウドの利活用を阻害する目的ではないことを理解しなければならない。概ね各ガイドラインが示すことは共通で、リスク管理機能が第三

者に委ねられることによって統制が弱まる、もしくは全く及ばなくなるリスクをいかに回避するかということだ。これは、重要業務を社外で運用する立場から言えば、至極当然のことである。

一つ例を挙げよう。

近年、シンガポールの金融機関が外部委託を増やす動きがあるなかで、MASは規制の改定を進めてきた。2014年にアウトソーシングガイドラインのコンサルテーションペーパー(協議文書)が提示され、コンサルティングファームとの協議、リーガルチェック、ベンダーとの調整などを経て、正式版がつい先日、2016年7月27日にリリースされた。

主な特徴は、「取締役会とシニアマネジメントの責任」と「外部委託のモニタリングとコントロール」についてさらにフォーカスしたことである。リスクアセスメントとデューデリジェンスの内容も、より明確に規定されている。

重要(material)な外部委託に関してはMASに事前通知を必要とし、金融機関はガイドラインの遵守状況をMASに説明できるようにしておく必要がある。このような厳格な委託管理を要求する背景として、金融ハブとしての国家を目指して規制を伝統的に強化していく風土がある。データの海外持ち出しについては、金融機関の要請を踏まえ、許容されている一方で、持ち出されたデータは自国内と同じレベルの管理を課すなど、情報漏洩防止に厳格な管理を要求している。

MASの求めるリスク管理実務（抜粋）

—概要
—取締役会とシニアマネジメントの責任
—リスク評価
—ベンダー評価
—外部委託契約
—機密性とセキュリティ
—ビジネス継続管理
—外部委託のモニタリングとコントロール
—監査と検査
—シンガポール国外への外部委託

—グループ内の外部委託

—内部監査の外部監査人への外部委託

外部委託先管理にこうした厳格な基準を規定しているため 、さらにガバナンスが効かなくなるであろうクラウドに、一層厳格な管理基準が適用されるのではとの懸念もある。クラウド利用に二の足を踏む金融機関が多く存在するのも事実だ。しかし一方で、MASはそのウェブサイト上で、金融機関の健全なクラウド利用を推奨し、当局として金融機関のクラウドの利活用にネガティブではない旨を明確に言及してもいる。こうした中で、クラウドを利用する側の金融機関、さらには一般企業にとって、具体的なリスク管理の項目が明確化されたことはむしろ喜ぶべきことだ。クラウドサービス事業者に対して何を求め、自社が何を行うべきか明確になった点で大きな進歩である。

4．セールスフォース・ドットコムの対応

クラウドに限らず外部委託全般として、システムの健全な運用を保証するためには前述の厳しいリスク管理は必要である。

話をクラウドに限定しよう。シンガポールや日本では、今まで曖昧模糊としていたクラウドのリスクがつまびらかになり、それに対する管理策がプリンシプルベースで明確なフレームワークとして提示された。金融機関など多くの企業がクラウドの利活用において明確な独自の自社基準を設けることがより容易になったのだ。多くの企業でこうしたリスク管理の方策が示され、対応するリスク管理の実践のもと、クラウドの活用が進んできたことは紛れもない事実である。しかし、それでも未だリスク管理を全てクラウド事業者に委ねようとするが故、リスクを定義しきれず二の足を踏んでしまう企業も存在している。

そもそもシステムの運用管理の責任は、金融機関に限らず企業側にある。業務の一部または全てを外部委託した場合（クラウド利用もこのケースに当たる）も同様である。どんなに委託先の事業者が堅牢なセキュリティでデータを保護しても、データを入出力する企業側の管理が甘ければ、重要なデータの漏洩は起こりうる。このことを理解したうえで、委託先としてクラウドサービス事業者を選択する必要がある。どこまでを企業側が行い、どこからを委託先のクラウドサービス事業者に求めるのか、これを企業側で明確にし、トータルで最高のリスク管理を実現していくことが望まれる。では、利用する企業側で正しくガバナンスが効いているという大前提のもと、セールスフォース・ドットコムが、リスク管理の方策を企業が自らの手で行うよりもはるかに堅牢に実施している点を具体的に紹介する。

繰り返しになるが、社会インフラとして非常に厳格なリスク管理を求められる金融業界、中でも一層厳しいとされるシンガポール金融当局のMASが定めるリスク管理項目を例とし、そのガイドラインが制定された背景とその意味、さらにセールスフォース・ドットコムの対応を述べる。なお、日本では金融庁がその検査の詳細について参照するFISCの安全対策基準の内容がほぼ同等である。しかし前述の通り、日本ではFISCの主催した有識者検討会でより詳細に規定された部分もある。そのため後半に項目を追加し、その対応についても合わせて記述する。

【概要】

金融機関が外部委託をする場合には、このMASガイドラインに書かれた内容について金融機関がReadyであることを示す必要がある。用意されたFormatに従って最低年一回、もしくは求めに応じて申告をしなければならない。場合によっては金融機関の外部委託をやめさせる、もしくは委託先を変えさせる権利もMASは持つ。これは当局としてのパワーを明示しているものだ。日本にはこうした内容は存在しないが、金融庁の検査などで指摘された金融機関の状況を見ると、同様の見えざるパワーを当局が発揮していることは間違いない。

【取締役会とシニアマネジメントの責任】

ガバナンス強化のため、取締役、シニアマネジメントの責任を明示している。従来に比べ、その説明責任も含め非常に重要視されている。この部分はコーポレートガバナンス、ITガバナンスの構築を企業が実践していくことであり、金融に限らず全ての業界において共通する。企業側で対応を求められる部分であり、サービス事業者が直接対応すべき内容ではない。

【リスク評価】

外部委託（クラウド利用）に求めるものをビジネス戦略上に定義する必要がある。まず有効なデューデリジェンスと、外部委託（クラウド利用）のアレンジメントがうまくいかなかった時のリスクを定義。この時社内にリスクを最小限にとどめることのできるリソースがあるかをあらかじめ確認しておく。そして

このリスクに対して外部委託（クラウド利用）することが、より利益があると判断できるかどうかを、分析しておくべきとされている。なお、この分析は些細な運用停止から大規模障害によるデータ漏洩といった甚大なリスクにわたるまで考慮しておくことが望ましいとされている。内容はあくまで、利用側の企業に求められているものであるが、正しくこのリスク分析を行うためには、評価のための情報公開が必要である。これに対し、セールスフォース・ドットコムは積極的な情報公開を行っている。クラウドについては先進的なテクノロジーであるが故に情報公開に対して消極的である事業者が多い中、オープンであることを是とするセールスフォース・ドットコムのアプローチは異質である。

【ベンダー評価】

外部委託先、特にクラウドサービス事業者はその実態がブラックボックスであることが多い。MASのガイドライン、日本でのFISC安全対策基準にもとづく金融庁の検査指針（金融検査に関する基本方針）、これらでもブラックボックスでの利用を認めておらず、十分な管理責任を求めている。つまり情報の開示に積極的でなく、後述する「立入監査を認めない」といった監査監督を妨げるような事業者は、選択すべきではないとしている。その他、サービスを利用する企業側の委託先事業者選択に際し、考慮すべき項目も明示している。信頼度や受託実績、財政状況、セキュリティ管理、内部統制、監査のカバーする範囲、リスク管理のフレームワークの有無と能力、BCP、DR、法制度遵守状況などがその項目である。セールスフォース・ドットコムでは、これらの求められる基準について全て準拠している。セキュリティやリスク管理については個別の項目として取り上げ、後述とする。少なくとも委託先の選択基準として事業者側に求められている内容については心配いただく必要はない。

【外部委託契約】

特にパブリッククラウド事業者では、提供するサービスは個別の顧客に対するものではなく、マルチテナント型の資源共有型の場合が多い。契約内容についても固定された共通のものを用意しているケースが多い。社会インフラでもある金融機関の業務では、求められるサービスレベルや内容が他の業界とは異なり、特別な項目やサービス水準を契約として受け入れる柔軟性が求められている。契約書の中に最低限含まれるべき項目について、ガイドラインでは定義をしている。外部委託範囲、パフォーマンス・オペレーション管理規定、機密性とセキュリティ、事業継続性、モニタリングと監査、インシデント時の報告と対

応、紛争時の解決、早期解約時処理、再委託先管理、適用法律などがその項目だ。これらが契約書に明記すべきとされているが、これはFISC安全対策基準についても同様である。こうした項目を契約書に文章として残したくないサービス事業者が多い中、セールスフォース・ドットコムのサービスはこれらの条件を満たし、必要に応じて契約書上への明記を約束している。

FISC安全対策基準で新しく追加された、かつMASのガイドライン上で強調されている項目について、セールスフォース・ドットコムの対応をもう少し詳細に記述しよう。

契約書に含まれるべき非常に重要な項目の1つは、「再委託先以下まで含めた監査権の確保」である。まずはメインとなるデータセンター（情報処理をする場所であり、データを保管する場所である）に対する立入監査権だ。特に金融機関に対し監督当局は、適切な監査とモニタリングを通じての管理を求めている。これを受け金融機関の多くは独自のセキュリティポリシーとして、委託先での定期的な実地監査を定めている。一方クラウド事業者は、マルチテナントの資源共有型のサービス提供であるがゆえ、セキュリティ上の観点という理由で立入を認めないケースが多い。もちろんセールスフォース・ドットコムは必要とする顧客に対しては立入監査権の受容を契約書上に明記している。事業者によっては、上記理由を盾に「外部監査レポートの開示を以って良しとする」主張もある。しかし勘違いしてはいけないことは、求められているものは「立入監査の権利」であり、実運用での監査方法はここでは触れていないことである。権利を明記した上で、実運用で最大限SOC２やIT7号などの外部監査レポートの利用をすることは、どのガイドラインも否定をしていない。実際、最新版のMASの外部委託に関するガイドラインでも、SOC2などの外部監査レポートが立入監査の実質的な代替となりうるとしている。しかし、金融機関固有のポリシーが全て外部監査によってカバーされていない場合（実際こういうケースの方がはるかに多いであろう）、金融機関は実際に現地に赴き、監査によって確認する。この条件を求めることも有り得、権利の明記はこうした場合の監査を妨げてはならないということを述べているのである。繰り返しになるが、セールスフォース・ドットコムもこの権利を認めた上で、実際は監査レポートなどにより実質の実地監査の頻度を減らせるよう顧客と打ち合わせている。

もう1つが再委託先管理である。データセンターに対するリスク管理責任については上述した。金融機関はこの責任をデータセンターへの監査とモニタリングで実現しているが、当局は同じ管理を再委託先以

下の外部委託先にまで求めている。重要業務を再委託、さらに再再委託していく場合、金融機関に委託先事業者と同等のリスク管理が求められる。セールスフォース・ドットコムは再委託先も含めた委託先を開示し、その上で重要業務や重要システムの外部委託と判断される場合、再委託先のリスク管理を保証している。実際には再委託先に対する立入監査の代替として、外部委託先であるセールスフォース・ドットコムが顧客と定めた契約と同等のリスク管理を再委託先以下に対して行う。再委託先以下に起因する情報漏洩などのインシデントが発生した場合は、その被害に対して全ての責任を賠償も含めセールスフォース・ドットコムが持つことを明記している。

【機密性とセキュリティ】

重要情報を預託する場合には、その情報保護は大きな課題である。特に個人情報を中心とするプライバシー情報の保護では、各国とも個別の法律により厳しい管理が求められている。MASのガイドラインでは、外部委託先が適切な方法で重要情報を扱い、管理していることへの確認が求められている。セールスフォース・ドットコムの情報管理体制は、ネットワーク層およびアプリケーション層の全てにおいて、機密性の確保のための十分な方策が施され、アクセス権の管理も含め万全である。またシステム的な暗号化やその他のデータ保護のテクノロジーについても間違いなく世界最先端のものである。詳細のプロセスについてはここでは割愛するが、Salesforceのセキュリティに関し、種々の白書が発行されているのでそちらも合わせて参照いただきたい。

【ビジネス継続性】

システム的な障害によってビジネスの継続が阻害されるというリスクに関しては、委託先事業者側のBCPが明確にあるか確認し、また思いがけない事業者のビジネス撤退など最悪のリスクを想定した計画を立案すべきである。

Salesforceのサービス基盤はすべてにおいて多重化を前提としており、データセンター自体も物理的に分離された形での複製をほぼリアルタイムで行っている。天災や大規模事故などでメインのデータセンターの業務継続が不可能になった場合でも耐性を保っている。更には顧客が手元にバックアップを持てるオ

プションも準備し、事業継続に対しても万全だ。またほとんど想定外ではあるが、万が一のビジネス撤退の対処時も契約上で明確に規定、細部まで安心していただける。

【外部委託のモニタリングとコントロール】

外部委託先のリスク管理を継続的にモニタリングし、定期的な監査による管理の必要性については契約の項で説明したのでここでは省略する。ただし、セールスフォース・ドットコムが必要な内容に関して受容の準備があることは改めて強調しておく。

【監査と検査】

監査に関しては、契約の中でその実地監査の権利を明記するという観点で述べてきたので本節では省略する。一点、当局の検査に対応することに関して言えば、監査と同様、重要業務を扱うシステムの外部委託では、必要に応じて実地検査を行う場合があり、委託先事業者はこれに対応しなければならない。この際、外部監査レポートでの代替などといったアプローチではなく、求められる通りの検査受容が必要となる。もちろんセールスフォース・ドットコムは当局の検査にも快く対応する。

【シンガポール国外への外部委託】

これはシンガポール独特の要求事項であり、国外に重要システムを外部委託する場合、もしくは重要情報を預託する場合の規定である。これらを国外に出す場合においてもMASの監督が及ぶように、明確にその委託先国の政策や法律に妨げられないことを保証するという内容である。Salesforceのサービスでは、データセンターが所在する複数の地域の中から、これを満たす先を自由に選択できる点で、準拠していると言える。

【グループ内の外部委託】

例として支店が本店のシステムを使うような場合、たとえ同じグループ内でも明確に外部委託契約を締結する必要があるという条項があり、特にプライベートクラウドをグループ内で構築し、グループで利用

するケースが想定されるが、Salesforceのようなパブリッククラウドの場合では、グループ外の事業者に委託をするという点で適用外である。

【内部監査の外部監査人への外部委託】

金融機関の内部監査業務を外部監査人に委託する場合には、外部の監査の妥当性を監査する際の独立性に課題が生じる。MASのガイドラインでは、外部の監査法人に内部監査業務を委託する場合、十分注意が必要であり、また金融機関の持つ会計監査法人に内部監査業務を委託すべきではないとしている。金融機関の内部マネジメントに関する項目であるので、セールスフォース・ドットコムの対応については省略する。

以上がMASの新しいガイドラインでリスク管理項目として定義されたものであり、セールスフォース・ドットコムはそのシステムの委託先としてリスク管理の統制が十分及ぶ対象である。事業者として非常に強固で堅牢なセキュリティ対策を行っていると同時に委託元金融機関（企業）の求めるリスク統制に対応している。

本項の冒頭でも述べたが、FISC安全対策基準で新たに追加された主な基準については、項目の観点ではMASの基準でほぼ網羅される。しかし、大項目としてクローズアップされ、新しい基準として定義されたもののうち主要なものも合わせてピックアップしてみたい。

【クラウドサービス利用にあたってのデータ漏洩防止策】

適切なデータ漏洩防止のための方策として、蓄積・伝送データの暗号化、暗号鍵の管理主体、暗号化の代替策について例示されている。セールスフォース・ドットコムの対応について言えば、データの暗号化では伝送データは現時点で最高レベルの暗号化を、蓄積データは必要に応じてオプションでソリューションを提供している（必ずしも全てのデータを暗号化することは、そのパフォーマンスの観点から最適ではないため顧客の選択可能なオプションとしている）。代替策についてもトークン化など例示されたものに関しては、ソリューションを提供するパートナー様のご紹介を通じ、必要に応じた実装を可能にしている。

暗号鍵は管理を金融機関が直接行うのではなく、非常に厳格な管理策によって事業者側で管理することで要件に合致、さらに各社のセキュリティポリシーにより暗号鍵を企業側で行わなければならない場合についても、オプションでソリューションを提供できる。同時に対応できるパートナー様のソリューションも紹介可能だ。

またデータ漏洩防止の観点で、記憶装置の故障などでは、ディスクを交換する際の確実なデータ消去が望まれる。当然であるが、これにも確実に対応していることを付け加えておく。

【クラウドサービス契約終了時のデータ漏洩防止】

資源共有型のクラウドサービスの場合、契約終了時にストレージのハード的な破壊や消磁によって特定顧客のデータを選択した消去ができない為、確実な論理的消去の方法が例示された。セールスフォース・ドットコムではこれらを確実に実行可能であり、追加的に顧客の求めに応じ、消去通知を発行できる。

おわりに

本稿では社会基盤として特に厳しいリスク管理を求められる金融業界におけるリスク管理の基準について取り上げた。その中でも厳しいとされるシンガポールの MAS の新しく発行された外部委託先管理のガイドラインと FISC で開催された有識者検討会を受けてリリースされた『FISC 安全対策基準』（第８版追補改訂）に示されたセキュリティ方策を解説。さらにセールスフォース・ドットコムの対応について述べてきた。このセキュリティガイドラインは、当然全ての業界に属する企業に共通の指針となるものと信じる。そしてセールスフォース・ドットコムではこれらの全てにおいて対応していることを改めて強調しておきたい。

クラウドの利活用に対して漠とした不安から消極的である企業にとって、これらのガイドラインとその対応が明確になった今、利用を妨げる理由はもはや存在しない。外部委託にせよ、その一形態であるクラウドにせよ、今までとは違ったアレンジメントで構築されるモデルに対しては、リスクを洗い出し、それに対して厳しく利用側で管理すべきと規制やガイドラインが出る。しかしこれを監督当局がネガティブであると疑心暗鬼になる必要はない。全てのガイドラインは明確にリスクを認識し、それらのリスクに応じて適切な方策を講じることを促しているだけなのである。

できるだけ多くの企業にクラウドの活用を促し、その成長と共に結果的に国益に資するものとなることを願ってやまない。

【筆者略歴】

株式会社 セールスフォース・ドットコム
インダストリー事業本部　スペシャルプロジェクト担当
榎　隆司

1981 年 IBM の製造開発部門に入社後、ハードウェアの製造開発に従事し、事業開発、インターネット決済、e-Business の普及などを中心に業務を行ったのち、クラウドコンピューティングのセールスフォース・ドットコムで、技術部門を担当。最近では金融機関のクラウド利用に関する有識者検討会を FISC の事務局として運営し、昨年、『FISC 安全対策基準』（第 8 版追補改訂）として、ガイドラインを刷新した。

なお、本稿の中での意見は、当社の公式見解ではなく、私見である。

また、関連法令等など信頼できると判断した情報に基づき作成されているが、法令・制度等の変更により将来変更になる可能性があることを付記しておく。