クラウドスペシャリスト・リレーインタビュー 第６弾「金融機関のセキュリティ要件」

クラウド
ICTシステム環境の最適化

「FISC安全対策基準」から見るNTT Comキャリアクラウドの取り組み

これまで導入には慎重と言われてきた金融業界においても、クラウドサービスの活用を始める機関が増えてきていますが、これにはどのような背景があるのでしょうか。また、顧客や第三者機関から求められる高い情報セキュリティ基準に対して、どのような対策をすればよいのでしょうか。

今回は、金融業界におけるクラウド活用の実態や今後の方向性、高度な情報セキュリティ基準を必要とする企業が、どのような点に注意してクラウドサービスを選定し導入すべきかをNTTコミュニケーションズ クラウドスペシャリストの藤本 広樹氏にお聞きしました。

NTTコミュニケーションズ株式会社
クラウドサービス部クラウドスペシャリスト
藤本 広樹氏

金融業界のクラウド活用実態

―　今や、金融業界でもクラウドの活用が進んでいると聞きますが、実際にはどのような状況でしょうか。

NTTコミュニケーションズ　藤本氏（以下、藤本）：

まず、クラウドサービスの利用に対しては、まだ慎重な姿勢を維持している金融機関が多いのではないでしょうか。その理由として、金融サービスの信頼性を担保するために、顧客情報等の機密性の高いデータの漏洩リスクにどのように対処するか、他の業界よりも厳しい法規制をどのように遵守するか、ということが、やはりネックになっていると思います。

とはいえ、営業支援システムや社内情報共有ツール、e ラーニングシステム、電子メール、インターネットゲートウェイといった「情報系システム」では、クラウドサービスを利用する金融機関も増えており、顧客情報と直結しないような 領域では、積極的にクラウドサービスを選択する方針を打ち出しているケースも多くなってきました。

また、最近の事例で、金融業界では聖域とされる「顧客データベース」や「取引先管理」などの顧客情報を取り扱う「業務システム」でもクラウドサービスを利用するようなケースもあります。

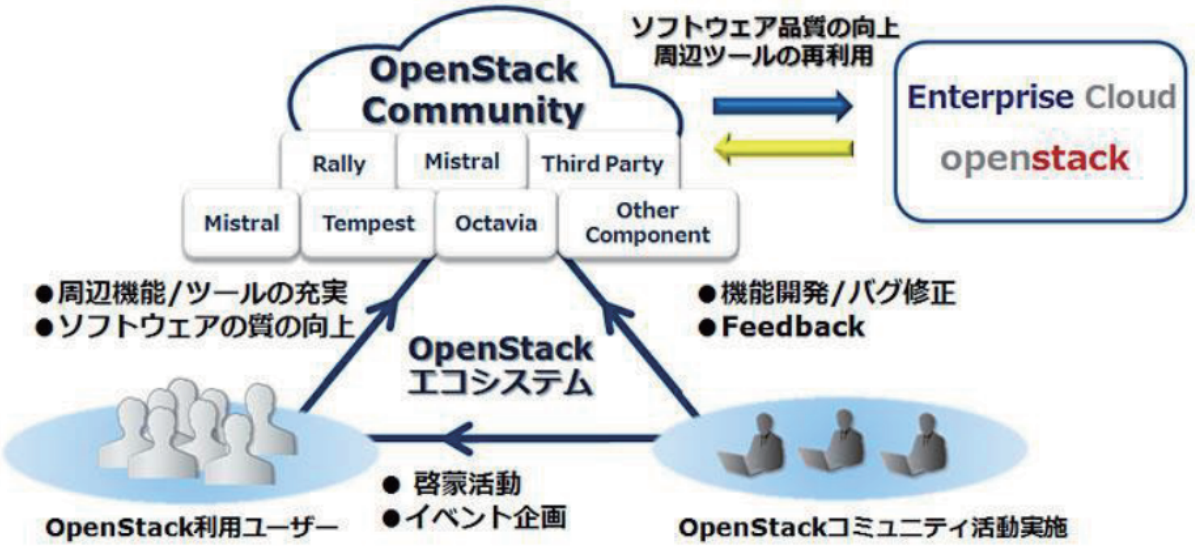

図1：「OpenStack」コミュニティ活動の背景と目的

クラウドサービス利用促進の背景とリスク管理

―　金融業界は、情報セキュリティ基準として、特に高いレベルを求められる業界だと思いますが、クラウドサービス利用促進の背景にはどのような事情がありますか。

藤本：

そうですね。金融機関の競争力強化のためのTCO削減が急務であることや最近のクラウドサービスの進化もありますが、金融業界でのクラウドサービス利用におけるガイドラインが明確になったことが大きな要因の一つではないでしょうか。

「金融情報システムセンター」(以下、FISC)という機関をご存じでしょうか。FISCは、銀行、証券会社、保険会社などの金融機関と通信・ICTの事業者で構成されている公的財団法人ですが、このFISCで2014年度に「金融機関におけるクラウド利用に関する有識者検討会」が開催されました。

この検討会が開催された背景には、「金融機関のクラウドの利用を健全に促進させ、より一層広げていくために、金融機関やクラウド事業者などの関係者間で、改めてクラウドのメリットやリスク、適切なリスク管理・契約管理のあり方を議論し、共通の認識と理解が必要である」という考えがありました。

つまり、金融機関が今後クラウドを活用するためには、金融機関ならびにICT業界がどのような対策をすべきか、ということが話し合われたのです。検討会には、代表的なクラウド事業者も数社参画したのですが、NTTコミュニケーションズは、唯一日系企業のクラウド事業者として参加いたしましたので、以下にその概要をご紹介します。

まず、FISCでは、クラウドサービスを大きく以下の3つに定義しています。

①単一の組織専用に提供される　「プライベートクラウド」
②多数の利用者で共用する　「パブリッククラウド」
③特定の複数組織間で共用する　「コミュニティクラウド」

クラウド事業者が提供するクラウドサービスは、すべて②「パブリッククラウド」というカテゴリに属すると定義し、またクラウドサービスを諸外国の金融監督当局での取扱いと同様に「外部委託の一形態」として扱うということで合意した上で、そのリスク管理対策をどうすべきかについて検討がされました。

検討会では、システムの可用性レベルとシステム上で取扱うデータの機密性レベルの組み合わせから、ITの領域を「コアIT領域」、「セミコアIT領域」、「ノンコアIT領域」の3つに分類し、各領域に求められる基準を洗い出してまとめたのです。

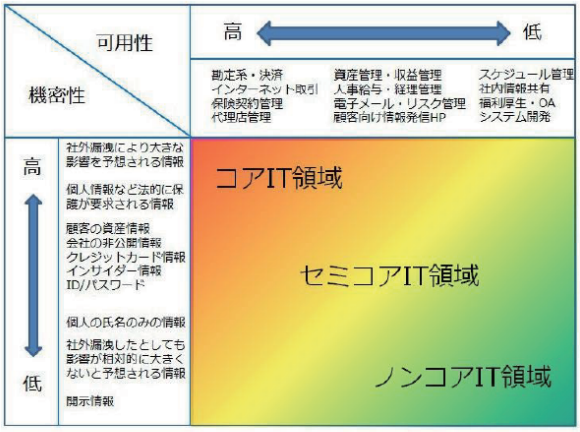

図1：クラウド利用におけるリスク管理の考え方

— 有識者検討会の結果、どのような指針が設けられたのでしょうか。

藤本：

FISCが発刊している「金融機関等コンピュータシステムの安全対策基準・解説書（通称：FISC安全対策基準）」が改訂されました。この「FISC安全対策基準」は、設備基準、運用基準、技術基準の3部で構成されており、金融システムの構築・運用における指針とされています。そして、有識者検討会の結果を受けて、2015年6月29日に第8版追補改訂版 が発表されました。

NTTコミュニケーションズの対応

— この指針に対するNTTコミュニケーションズの見解を教えてください。

藤本：

第一に、NTTコミュニケーションズは電気通信事業者として、「電気通信事業法」を遵守する責務があります。特に、「旧第一種電気通信事業者」に該当する通信設備・機器を保有しているため、安定したサービス供給という観点では、これまでも法的拘束力のある環境でサービスを提供してきました。あわせて、様々な外部認証を積極的に取得しながら信頼性の高いサービスを長きにわたって提供してきた実績もあります。

このように、法的拘束力と外部評価に裏付けされたNTTコミュニケーションズのクラウドサービス「Enterprise Cloud（通称：ECL）」は、「FISC安全対策基準」の第8版追補改訂に対しても準拠していることが確認されており、結果として現在まで多数の金融機関に採用して頂いています。

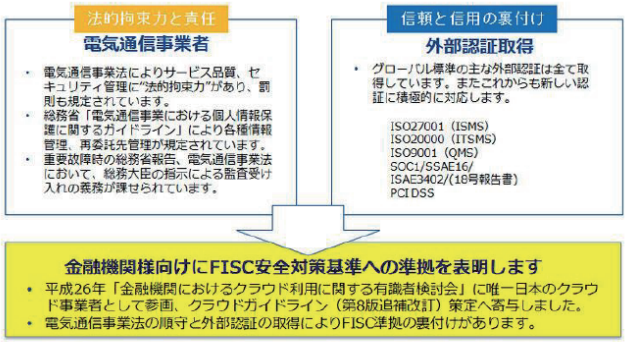

図2：NTTコミュニケーションズの「FISC安全対策基準」に対する姿勢

— それでは、FISCの安全対策基準「第8版追補改訂」の注目すべきポイントを教えてください。

藤本：

そうですね。特徴的なのは「再委託先管理」「データ漏洩防止」「立入監査」そして「サイバー攻撃対応体制の整備」ではないでしょうか。

①再委託先管理：
クラウド事業者に対し、クラウドサービスの公開情報に加え、非公開情報の開示を求めて、リスク管理の状況等を評価することになっています。

ここでは、一般的な契約内容の確認に加え、特徴的な点として、再委託先管理の確認があります。有識者検討会で、クラウドサービスは「外部委託の一形態」として扱われることとなり、さらには、金融機関の再委託先で情報セキュリティに関連した不祥事が発生していることから、クラウド事業者にも再委託先管理を徹底させることになったようです。

この点、NTTコミュニケーションズでは、総務省「電気通信事業における個人情報保護に関するガイドライン」第12条に基づいて従業員および委託先の監督が法的に義務づけられていることを評価いただいています。

②データ漏洩防止：
まず、データの取扱いについて、クラウド事業者の責任範囲を明確にする必要があると考えます。

基本的には、利用者がクラウドサービスへ収容したデータに関しては、利用者側の責任範囲となり、内部犯行による情報漏洩対策の観点からも、重要データを暗号化等で保護し、契約終了時にはデータ消去をする必要があります。またクラウド事業者側ではディスク等の電子媒体の取扱いに関して厳密な運用がされなければなりません。

NTTコミュニケーションズは、総務省「電気通信事業における個人情報保護に関するガイドライン」第３章（各種情報の取り扱い）や第１０条（保管期間等）の規定を遵守し、適切な方法で運用していることをお約束しています。

③立入監査：
よく話題になるのが立入監査ですが、クラウド事業者によっては受け入れが難しいケースもあります。しかしNTTコミュニケーションズでは、コアIT領域に関して、監査対応範囲を明確化した上で、条件付きで立入監査の受け入れを行っています。また電気通信事業法において、総務大臣の指示による監査受け入れの義務が課せられているという背景もあります。

④サイバー攻撃対応体制の整備：
これはクラウドサービスに限ったことではありませんが、近年の金融機関に対するサイバー攻撃の多発を背景に、特に直接の内部統制が及びにくいクラウド事業者の対応力を知ることは重要な要素としてあげられます。

NTTコミュニケーションズは、サイバー攻撃に対して、独自のセキュリティオペレーションセンターによる監視、セキュリティベンダー研究機関との連携、NTT-CERT活動による情報収集、インシデント発生時の全社災害対策体制が確立されています。

― 他に、クラウドサービス利用で注意すべきことがあったら教えてください。

藤本：

クラウド事業者との責任分界点の明確化です。一般的には、OSより上位のミドルウェアやアプリケーションが利用者側の責任範囲になり、クラウド事業者はシステム基盤側とされています。これは、データ管理がどちらの責任範囲かという観点によるもので、利用者とクラウド事業者との事前の確認と合意が必要となります

また付け加えるなら、システム基盤側にもハードウェアの設置場所であるデータセンター、ネットワーク（回線）部分が存在し、それぞれに対してクラウド事業者として確実に統制が取れるのかを見極めるべきでしょう。

NTTコミュニケーションズのクラウドサービス（ECL）は、自社のデータセンター、ネットワーク（回線）を基本としているため、障害時や不測のセキュリティ事故、災害時においても一社で統制を取ることが可能で、それは東日本大震災時の計画停電時の対応で実証されています。

― それでは、利用者が「FISC安全対策基準」の準拠状況を知るにはどうすればよいでしょうか。

藤本：

NTTコミュニケーションズでは、改訂版で追加された項目も含め、準拠状況をまとめた一覧表を作成していますので、要望を頂ければご提供いたします。

FISC安全対策基準第8版追補改定						NTT Comクラウドの対応				利用者側対応
大項目	中項目	項番	小項目	適用にあたっての考え方	必須レベル	準拠状況	ECL1.0の見解と実施内容	参照する外部認証	NTT Comドキュメント	対応要否
（Ⅲ）運用管理	3.オペレーション管理	運 19	オペレータの資格確認を行うこと。	コンピュータシステムの不正使用を防止するため、オペレータの資格確認を行うこと。	◎	○	本サービスのオペレータの物理的入退館管理および本サービス及び運用管理システムへのアクセス権限管理について、必要な管理手順を明確にし、資格を付与しています。 （ISO27001附随書A9.2：利用者アクセスの管理） （ISO27001附随書A11.1：セキュリティを保つべき領域）	ISO27001	物理環境管理規程 ECLアクセス管理ルール（SOP文書）	

図3：「FISC安全対策基準」への準拠状況一覧表（抜粋）

― NTTコミュニケーションズでは、「FISC」以外の外部認証の取得状況は、どうなっていますか。

藤本：

もちろん、品質やセキュリティに関する外部認証も継続して取得しています。例えば、今年制定され、クラウドセキュリティに特化した認証であるISO27017に関しても取得予定となっていますし、これからも新しい認証取得に向けて積極的に対応していきます。

目的		規格／指針
セキュリティ管理	適切なセキュリティ管理の実施	ISO27001（ISMS）
	クラウドサービスの情報セキュリティ規格	ISO27017（※2017年取得予定）
	個人情報の保全	JIS Q15001（P mark）
品質・安全性管理	ITサービスの適切な品質管理	ISO20000（ITSMS）
	サービス提供に対する品質管理を認証	ISO9001（QMS）
内部統制	内部統制の有効性確認	SOC1/SSAE16/ISAE3402/(18号報告書)
情報管理	クレジットカード情報の保護	PCI DSS
事業継続	事業継続	ISO 22301（BCMS）
総合評価	金融系品質・セキュリティ管理	FISC安全対策基準（8版追補改訂版）
	安全・信頼性に係る情報開示	ASPIC「クラウドサービスの安全・信頼性に係る情報開示認定制度」

図4：Enterprise Cloud 外部認証取得状況および方針
（※一部リージョンは今後取得予定）

藤本：

NTTコミュニケーションズは、電気通信事業者の実績と強みを活かし、引き続き金融業界を含む高度なセキュリティ基準を持つ企業さまにも安心してご利用いただけるクラウドサービスを提供してまいります。

サービス紹介

≫Enterprise Cloud

安定したサービス供給で信頼性の高いサービスを長きにわたって提供してきた、NTT Comのクラウドサービスである「Enterprise Cloud」は、「FISC安全対策基準」の第８版追補改定にも準拠し、多くの金融機関に採用されています。

Enterprise Cloud

NTTコミュニケーションズ株式会社 クラウドサービス部
公式サイト：http://www.ntt.com/enterprise-cloud