加藤 俊直氏

堤 順

# 金融×IT対談


あらた監査法人
システム・プロセス・アシュアランス部
パートナー

株式会社野村総合研究所
ERM事業企画部長


Profile/Toshinao Kato

1995年 大手外資系コンサルティング会社入社。2003年 国内系コンサルティング会社立ち上げを経て、2006年より現職。主に、J-SOXアドバイザリー、システムリスク管理態勢構築、大手ITベンダーや信託銀行をはじめとする数多くの委託先の外部委託先監査、各種金融機関システム委託先のサービスレベルマネジメントスキームの構築を手がける。公認会計士、システム監査技術者。

Profile/Jun Tsutsumi

1991年 野村総合研究所入社。証券会社向けトレーディングシステム開発に従事。96年から2000年まで、NRIヨーロッパに出向し、現地日系証券会社の基幹系システム再開発プロジェクトに参画。2003年から2006年まで野村證券に出向。2006年よりリスクマネージメント、ITガバナンス等のコンサルティングに従事。2011年5月より現職。

**近年、個人情報漏えい事件が相次いでいることもあり、金融機関の内部統制に対する意識がなお一層高まっている。中でもシステム委託先に対する管理は大きな課題だ。委託先を有効に管理するためのポイントは何か、委託先の内部統制に対する第三者保証はどのように活用されているか。これまで数多くの金融機関の委託先監査に当たってきた、あらた監査法人の加藤俊直氏に語っていただいた。**

## 業務委託先を有効に管理するためのポイント

**堤**　近年、個人情報漏えいの事件が相次いでいることもあって、金融機関では内部統制に対する意識がなお一層高まっているように感じています。個人情報漏えい以外にも、サイバー・セキュリティをどう確保するか、クラウド化にどう対応するかといった課題もあり、金融機関のシステム部門では問題が山積しています。

御社にもさまざまな相談が寄せられていると思うのですが、加藤さんはどの辺りに注目していますか。

**加藤**　2014年を振り返ると、やはり個人情報漏えいや顧客情報悪用の対策の相談が多かったと思います。また、もっと幅広く「顧客情報に関連するシステムの管理体制を総点検したい」という話をいただくケースもありました。

そうした相談は金融機関からだけではなく、金融機関のシステムを受託している企業からも多く受けました。受託先であるITベンダーからは、「これまでは金融機関ごとに個別に対応してきたけれども、どの金融機関に対しても共通のメッセージを出していけないか」といった相談

もありました。

**堤**　NRIのような金融機関から委託される側にとって、情報漏えいを起こさないための対策を取ることはもちろんのこと、「そうした対策によっていかに内部統制がしっかり行われているか」説明責任を果たすことも大事です。そうしたときに御社のような監査法人に「保証」という形で説明責任の力を引き上げてもらえるのは非常に助かります。

**加藤**　確かに、客観的な第三者として、対策の有効性を保証できるのは、監査法人の保証業務ならではないかと思います。もちろん、実際に取り組むのは企業、金融機関自身ですが、「本当にそれができているのか」という疑問に、運用状況まで含めた形で「大丈夫ですよ」と伝えられるのは、社会的意義のあることだと思います。ぜひ、監査法人を有効に活用していただきたいと思います。

ところで、昨年金融機関のリスク管理全般において特に注目されたテーマは委託先管理でした。

顧客情報を悪用した事件も実際には委託先で起きたものでした。委託先管理のポイントを一言で言えば、「ガバナンスが効いているか」ということになると思います。しかし、それを具体的にどう確保するかとなると、簡単ではありません。例えば、委託先との間でサービスレベルを決めていたとしたら、それをどのように順守してもらうかといった問題は必ず出てきます。

**堤**　NRIが金融機関から委託を受ける場合、1次委託先となることが多いです。しかし金融機関が把握したいのは、1次委託先だけではなく、再委託、再々委託、末端まで、というのが最近は普通になっています。われわれとしても、こうした要請を真摯に受け止めて、末端まで把握するよう努めていかなければいけないと考えています。

**加藤**　内部統制というとガバナンスの観点もありますが、一方で反社会的勢力への対策の面もあるので、ある程度は末端までの情報が必要になってくると思います。

**堤**　そうですね。ただ、これは日本の特殊事情なのかもしれませんが、ソフトウエア業界というのは階層がかなり深くて、再委託、再々委託の先に個人事業主の方を雇っていたりするケースが少なくありません。それをリアルタイムで把握するのはかなり難しいことです。

われわれとしては、リスクに鑑みて本当に末端まで把握しなければいけない業務は何なのかを確認して、そこを集中的に監督するようにしていかないといけないと考えています。

**加藤**　委託先にはITベンダーだけではなく、いろいろな業務を行っている会社があります。したがって、委託先を管理するにあたって、まずは全体像を整理する必要があります。委託先でどういう業務が行われ、それぞれどういうリスクがあるのかを整理していくと、自ずと、重点管理先なのかどうかが明らかになってくると思います。

**堤**　以前、御社に金融検査の模擬検査をやっていただいた時に、「ハードウエアの廃棄業者は末端まで把握していますか」と聞かれて驚いたことがあります。われわれは開発業務を行っていますので、それらの委託先については非常に気をつかっていたのですが、廃棄業者については盲点になっていたということがありました。

**加藤**　委託先の管理は、全社レベルの仕事だと思っています。企業規模が大きくなると部門ごとに対応しがちですが、そうすると部門をまたがる業務などは見えなくなってしまう可能性があります。その辺りを全社レベルでシームレスにカバーできれば、適切な管理ができると思います。

## 委託先の内部統制に対する2種類の第三者保証

**堤**　委託先のリスク管理や情報セキュリティ態勢などの内部統制が整備されていることを第三者が保証する基準として、財務報告を主目的とした報告書（米国基準：SSAE16、日本基準：86号）[注1]と、より幅広いシステムリスクの統制を包括的にカバーした報告書（米国基準：SOC2、日本基準：IT7号）[注2]があります。

金融機関が委託先にこうした第三者保証を受けることを要求するのは、欧米などでは非常に一般的になっていますね。

**加藤**　はい。欧米では「第三者保証を取るのが当たり前」になっており、委託先を決めるときの必要条件になっていると思います。日本ではまだそこまで強くは求められていない印象があります。

**堤**　日本では、取っていることが、条件としてプラスに働く感じでしょうか。

**加藤**　そうですね。SSAE16は会

計監査、内部統制監査に使われるので、強制的とまでは言いませんが、SOC2に比べると、より使われている状況だと思います。SOC2は監査そのものに使うわけではないので、日米における認識に大きな違いが出ているのだと思います。

**堤**　日本でも第三者による評価は、業務委託の提案依頼書（RFP）の条件になりつつあります。やはり、「第三者による点検」はわかりやすいのだと思います。大手の金融機関からも求められますが、どちらかと言えば彼らは自ら確認する傾向が強いように思います。もしかすると地方銀行の方が第三者による評価を重視しているかもしれません。

**加藤**　地方銀行は内部監査やリスク管理に割ける資源がある程度限られていますので、その限られた資源の中で適切にシステムリスクの状況を見なければなりません。ですので、効率的な仕組みがあるならば、利用するニーズはあると思います。

**堤**　こうした保証の取得は、われわれ委託先にとってはそれなりの負担になります。

**加藤**　委託先にとっては、いろんな金融機関から監査に入ってこられることを考えたら、むしろ1回で済むほうがトータルでは効率的かもしれませんね。

単に準拠性を形式的に「○」「×」とチェックするだけなら簡単なのですが、監査においては、「本当にリスクを低減できているのか」という観点で評価する必要がありますので一筋縄ではいきません。管理体制が単に形式的に整えられているだけではないかどうか、監査、評価ではその辺りに気をつけています。

**堤**　当然のことですが、毎年、同じ視点で監査をしても意味がないわけです。われわれは毎年、監査法人に見てもらう前にNRI社内で内部評価をやっています。その際も、評価計画を立てる段階で、経営と「今年のリスク評価はどこに着眼するのか？」議論するようにしています。「今年は障害が多かった」とか、「取引量が増えた」とか、着眼点のリストを洗い出して、そこの部分はリスクが高まっているので厳しめに見ないといけない、ということを話し合うわけです。

**加藤**　委託先は自社の状況を、金融機関などの委託元ともっと共有していった方がよいと思っています。委託先のシステムがどのような状況なのか委託元に把握してもらうことで、第三者評価の結果についても、より理解してもらいやすくなりますし、金融機関自身も、当局などに説明しやすくなると思います。

## SOC2報告書をどう活用するか

**堤**　先ほどSSAE16の方がSOC2に比べて利用が先行しているというお話がありました。しかし、SSAE16は財務報告を目的としているので、例えば、情報漏えいを起こさないための機密性を保証するにはそぐわないものだと理解しています。SOC2の枠組みでの監査がもっと活用されるべきだと思うのですが、いかがでしょうか。

**加藤**　システムの信頼性の内部統制を保証するサービスとして、米国やカナダで基準化された「Trustサービス」を使った評価制度もありましたが、システムリスクに関連する保証が必要な場合でもSSAE16の前の制度にあたるSAS70を利用するケースが圧倒的でした。

SAS70やSSAE16の対象は財務報告に関連する統制と限定されているため、情報システムのリスク管理について評価、保証する場合には、SOC2あるいはその日本版のIT7号を使ったほうが目的に合致していると思います。

**堤**　NRIでもデータセンターはSOC2を取得しており、これを拡大することを考え始めてはいるのですが、SSAE16ほど有名ではなく、金融機関にも浸透していないことから、状況を見ながら対応していくべきか考えているところです。

**加藤**　NRIがSOC2報告書を作ることによって、委託先に依頼している業務のシステムリスク管理状況について、理解を深めて頂けるとよいですね。

**堤**　そうですね。

ただSOC2の利用法には、まだまだわかりづらいところもあります。例えば個人情報保護については、いくつかの省庁からかなり具体的に安全管理措置のガイドラインが発表されています。日本の金融機関

は委託先にそうした安全管理措置を守っているか確認する際に、米国発のSOC2の枠組みを使って説明を求めるということで、整合性は取れるのでしょうか。

**加藤**　その点については、「整合性は取れる」と思います。確かにSOC2はTrustサービスの原則と規準がベースになっており、各省庁から出されているガイドラインそのものに合致しているわけではありません。そのため、ITベンダー側も「SOC2を取りました」と主張するだけでは不十分で、SOC2などの枠組みを活用して、各省庁の求める管理水準を第三者から見てもクリアできていることを説明していく必要があると思います。

これは、委託元の金融機関についても同じことがいえます。第三者保証報告書の内容が、自社・自行のリスク管理水準と100%一致していることはなかなかありません。委託元は、「第三者保証報告書でどこまでカバーできているのか」、「他に足りないところはないか」、「委託先とどういう形でコミュニケーションしていけばよいか」といった点を主体的に検討していくことが求められていると思います。

## マイナンバーに民間業者はどう対応するか

**堤**　話は変わりますが、いよいよ来年1月から共通番号、いわゆる「マイナンバー」が始まります。金融機関ばかりでなく事業者も、どのように安全管理措置を講じているか、消費者や利用者にアピールしていかなければいけないわけです。御社でもマイナンバー関連の相談は増えているのでしょうか。

**加藤**　「個人番号関係事務実施者」となる事業者が多いですが、安全管理措置をどう守るかというよりも、個人番号自体をどう取り扱えばよいか、という観点の相談が多いように思います。特定個人情報保護ガイドラインや安全管理措置における個々の項目の対応を考える前に、まずは自社における個人番号・特定個人情報の管理態勢を確認することがポイントだと考えています。

特定個人情報、すなわち個人番号の保護状況に関する評価については、行政機関や地方公共団体、情報提供ネットワークシステムを使用した情報連携を行う事業者などに実施が義務付けられますが、その他の事業者については義務付けられておらず、実施するのが「望ましい」という表現になっています。現時点では、多くの金融機関が評価する方向に進むと考えています。

ただ今回も、先ほどから出てきているような「保証」まで求められるのか、それとも、現状でどの程度までできているかの「評価」にとどまるのかは、今後社会的なニーズを鑑みつつ、クライアントとも相談しながら決めていければと思います。

**堤**　保証まで求めない場合でも監査法人に見ていただくことは可能ということですか。

**加藤**　はい。目的に応じた方法で評価することはもちろん可能です。

**堤**　まずは評価だけしてもらって、世の中の動きを見ながら保証に格上げするかどうか決めるといったアプローチも可能ということでしょうか。

**加藤**　はい。保証するためには規準が必要です。当然、評価するときも物差しは必要ですが、保証になるとその規準が「目的に合っているか」「完全なのか」などの、規準の適切性もより必要になります。

**堤**　なるほど。むやみに厳しくなり過ぎてもいけないので、こうしたアプローチも選択肢の一つかもしれませんね。

マイナンバーへの対応は、間近に迫っているため、息つく暇もなく物事が進んでいます。われわれも、お客様のご要望や、国の要求水準を見ながら対応を進めていきたいと思っています。今後もぜひいろいろ相談させてください。

本日は貴重な話をありがとうございました。

（文中敬称略）

---

（注1）SSAE16保証報告書：
米国公認会計士協会が公表したガイダンスに基づいて、受託会社の財務報告に関連する内部統制を評価した報告書のこと。

（注2）SOC2保証報告書：
米国公認会計士協会が公表したガイダンスに基づいて、受託会社のセキュリティ、可用性など会計報告以外の内部統制をTrustサービスなどの基準で評価した報告書のこと。