講演レポート

クラウドサービス利用時のカスタマ認証取得の重要性

稲垣隆一法律事務所　　弁護士　稲垣　隆一氏

■経営、リスク、責任の概念

ISMS は経営にどう役立つか、または経営が目指すものにどう役立つのか。

弁護士の体験から見た経営とは「リスク処理」である。経営はリスクへの挑戦であり、そのためにリスクの測定、対応、評価をして、リスクを取り除くものである。経営としてさまざまなリスクを測定し、どう扱うべきか、企業の社会的責任、評価が法的リスクにどう影響するか－つまり経営は法的リスクを把握したい欲求に常にかられているのである。

では、経営は法的リスクとして何を知りたいのか？　経営は、責任を発生させる原因の事実、たとえば、パンデミックによる従業員の罹患率が生産性にどう影響し、取引先もビジネス供給ができなくなることによる代金回収困難、損害賠償請求など、正規の要求ができなくなることの事実を見極め、ガバナンスし、マネジメントすることで法的リスクをマネジメントすることになる。

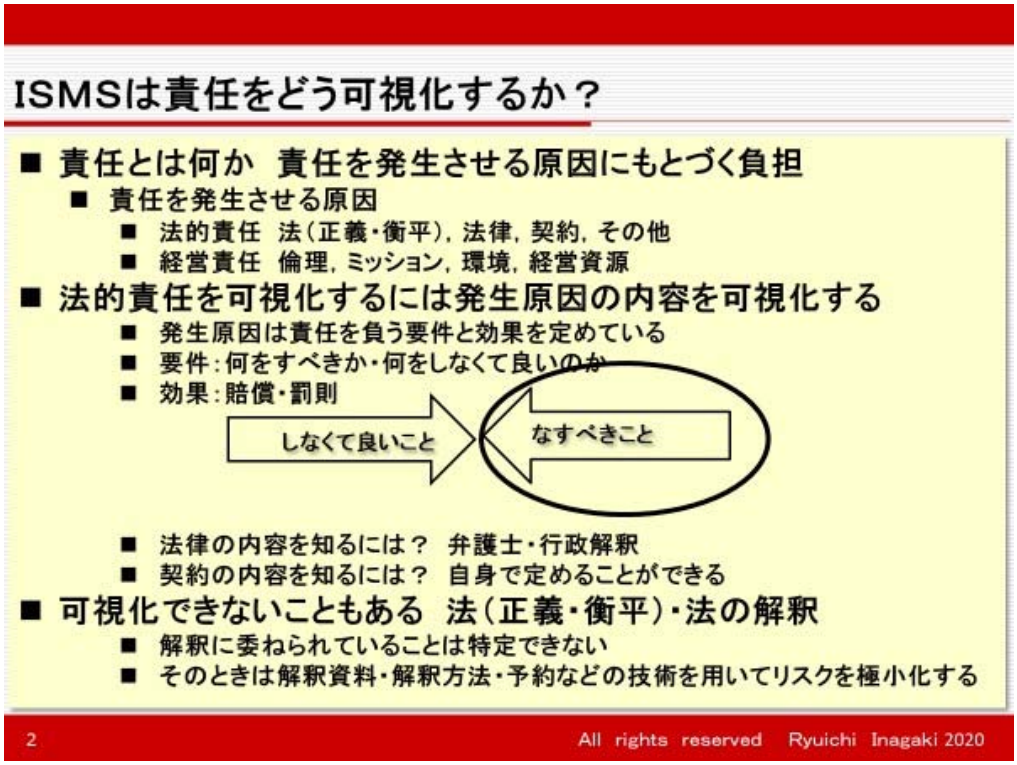
■ISMS は法的リスクの可視化に役立つ

では、ISMS はこうした法的リスクの取扱いにどう役立つのか。

自社と連携会社、クライアント間でのサプライチェーンについて、責任の発生原因を根拠づけるために法律や契約がある。たとえば、セキュリティに関する守秘契約、営業秘密保持、個人情報保護義務や規範で相手企業に対する自社の責任発生原因が定められており、情報漏えいがあった場合には自社側の責任範囲や対処方法、賠償の内容等が規定されている。

法的リスクとは、責任発生原因事実の存在と残存に関するリスクのことであり、経営側は法的リスク把握のために事実発生の可能性を知りたいのである。ここでいう事実とはセキュリティの問題、技術問題におきかえると、セキュアなシステム、セキュアなネットワークを構成する技術、企画～開発～保守～運用の的確さ、調達の最適性、データ管理などの問題がある。想定どおりに動くのか、可用性が維持できているのか、データはセキュアな状態で完全性が維持できるのか、などである。最終的に責任の発生原因となる情報資産のセキュリティレベル、残存リスクは、ISMS によるリスクアセスメントで把握

でき、これによって責任発生原因事実の特定・明確化が可能となる。つまり、ISMS はリスクマネジメントを通じて経営の法的リスクを知りたいという欲求を満たすことができるのである。



上に述べたことは証拠にもとづいている。法曹にとって「証拠なき主張は無」である。私も法曹の端くれ。私の認識は正しいか？証拠が欲しかった。そこで私は、平成 15 年に主任審査員資格をとり、平成 17 年には事務所で ISMS 認証を受けて、身をもって証拠収集した。

やってみてわかったこと。それは ISMS の中核はリスアセスメントであり、経営者に対し、セキュリティに関する事実・技術・法的リスクに関する合理的な資料を提供し、経営を支える枠組みだということであった。脅威をマネジメントすべく、徹底したリスクアセスメントを行い、ベストプラクティスの意味を突き詰め、有効な対処策を厳しくかつ合理的に選択することは、法曹が、妥当な結論を得るために徹底して証拠を収集評価し、裁判所に的確な準備書面を提出するという訴訟活動と同じであった。私は、ISMS の更新を繰り返すなかで、ISMS を維持するための徹底した取り組みが、訴訟リスクに耐えうるセキュリティ対策のために極めて有効であることを確信した。

ISMS を真面目に構築・維持することは訴訟上のリスク回避に対応できる非常に効果的な方法と考える。ISMS の特徴であるセキュリティマネジメントは、経営のミッション、目的から、対象と実現すべきセキュリティレベルを論理的な結論として設計し、合理的なリスクアセスメントを行うことで、セキュリティに関する経営リスクが適切に把握できる枠組み・視点を持っている。そのため、リスクアセスメントを徹底的に行うことで、合理的な有効性のある対策を講じ、残存リスクを把握できる。厳しさを持ったアセスメントを行っていれば、もしも訴訟上でどんな主張があったとしても、過失や監督義務を基礎づける、結果の予見可能性や回避可能性について、証拠をもって主張・反論ができる。事故等が発生した場合にも、計画を的確に予定どおり実践できる。さらに PDCA を回すことによりレベルの向上が図れるのである。

ISMS は情報資産を対象としたセキュリティマネジメントではあるが、ISMS 構築によるリスクと責任の可視化や、継続

的な運用によって可視化の精度向上が実証できる。ISMS 認証は、ISMS を構築・維持している受審企業の立ち位置を的確に相手企業に示すことができ、不断にそれを向上しようとしている企業であることを証明できるのである。

■クラウドは外部委託と同じリスクを持つ

クラウド利用の問題点は、仮想化技術を誰が、どこで運用するのか、どのレベルで誰が責任をもって運用するのか、である。他者のクラウドを利用すれば、国を越えて自社の情報資産を外部委託する場合が出てくる。その際、セキュリティ体系、つまり、何か発生した際に、どの国で、どの法律を適用して裁判を行うのか、が問題となる。近代国家においては、裁判の結果を受けた差押え行為等は国の機関でなければ執行できない。裁判にあたってはその国の法律家に任せざるを得ず、高いリーガルコストを強いられる可能性があるため責任追及が難しくなる。

つまり、クラウドの問題は基本的には外部委託と同じと考えられ、外部委託の責任問題がありとあらゆるところで発生する。社会的に大事な事業、たとえば、鉄道、医療、電気などは、法律に基づき、事業の許認可、取扱者の資格・教育システム、機器・システムの規格、検査・監視、保守サービスシステム、それを支える様々なベンダーの存在など、重層的な事業や業務の品質を保証する仕掛けがあるのに対し、クラウドにはそのようなシステムもなく、継続性についてはクラウド事業者に任せざるをえなくなる。さらに暗号に関する国の権限、扱いも異なる。今クラウドが論じられているのは、クラウドに関する社会制度の未熟さや、未整備の状況が問題視されているのである。このようなリスクをどう扱うべきか、最低限の対策として何をすべきか、サプライチェーンの中にどう寄与すべきかを考えることが重要なのである。

■クラウドの法的リスク対応

クラウドの法的リスクについては責任の発生原因を特定し、発生の可能性を伝えることが重要である。セキュリティ侵害のアセスメントをし、対策を講じ、残存リスクを正確に把握していることの認証を受けたうえで事実を伝えることが正確なリスクコミュニケーションに役立ち、企業間のサプライチェーンの意思決定の際に重要となる。

法的リスクを生じさせる事実を知りたければ、設定したセキュリティレベルに達しない原因を作るセキュリティリスクを把握する。もし自分で把握できなければ、コンサルタントや ISMS 認証やセキュリティ監査も大事な情報提供となる。セキュリティリスクとしてどれほどの粒度で知りたいのか、認証登録証でいいのか、セキュリティ監査報告書レベルか、監査調書、是正記録まで求めるのかは、取引によりさまざまである。

ISMS 認証の場合は、認証更新回数、審査報告書の提出を指示することも可能である。また、サプライチェ―ンのリスクコミュニケーションにより主体間の信頼の維持・強化にも役立つ。認証の更新によって、さらに精度が高まり、サプライチェ―ンの中で責任の発生原因の存在可能性（リスク）に関する情報を共通の言葉で流通させることができる。

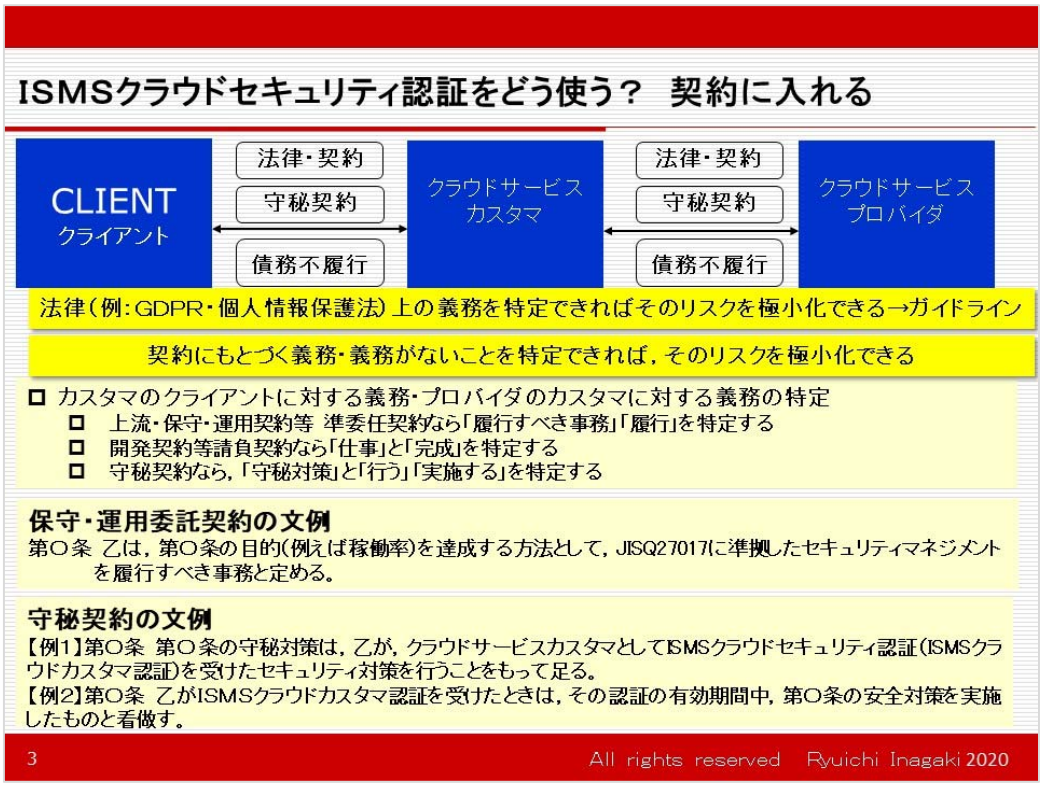
■ISMS クラウドセキュリティ認証の活用

ISMS クラウドセキュリティ認証は ISMS 認証を前提に、クラウドサービスの提供・利用に関して認証する、ISMS の拡張認証である。その認証基準のベースである ISO/IEC 27017 にはカスタマ、プロバイダ別になすべきことが規定されている。カスタマとプロバイダが連結された視点でつくられている点は有益である。また、サプライチェーンを前提としたネットワークについて自社のなすべき事項が明らかになっている、という点で、従来の ISMS 規格とは異なっている。

ISMS の認証基準である ISO/IEC 27001 では、企業の事業特性に応じたセキュリティの構築・実施、法令や契約遵守（の仕組み）を要求しており、組織単体のセキュリティマネジメントとして普及してきた。

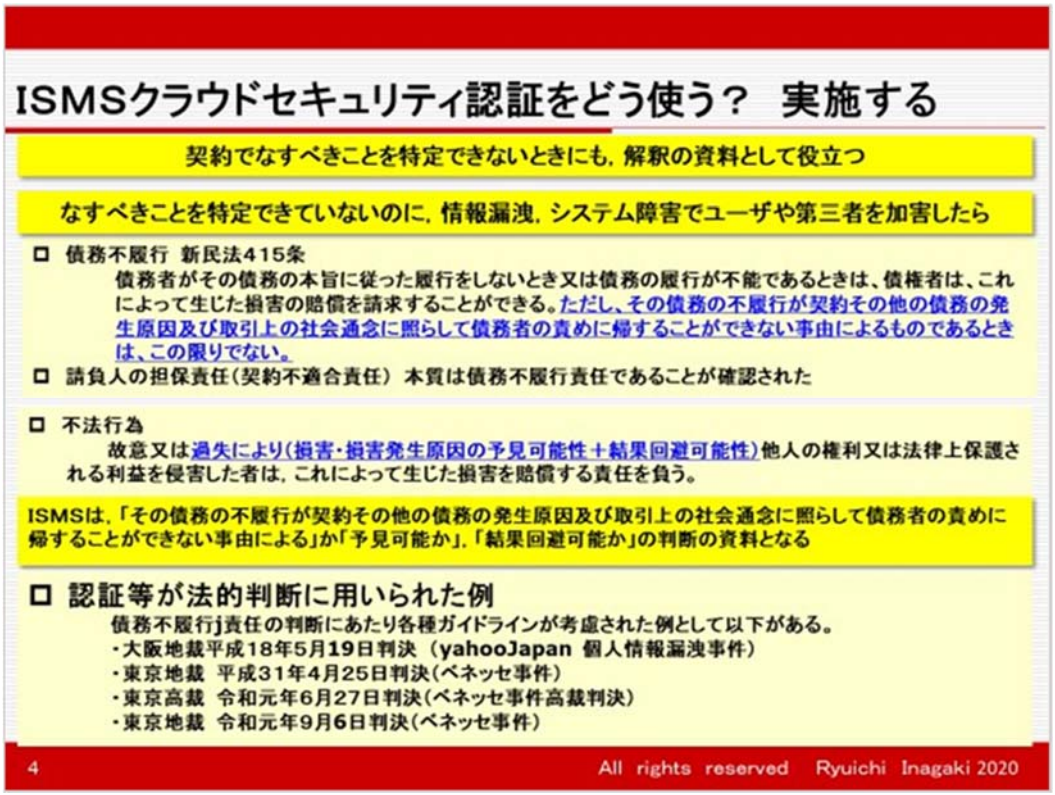
一方、ISMS クラウドセキュリティ認証基準のベースである ISO/IEC 27017 は、クラウドサービスのサプライチェーンの中でなすべきことを定めた ISMS を前提としたクラウドサービス固有の規格としてつくられている。この規格は社会の成熟に伴って本来なすべきことをまとめた、日本発の、現実的で使いやすい規格である。

ISO/IEC 27017 に基づいて法的環境を整備すると、法的リスクの軽減に役立つ。ISMS クラウドセキュリティ認証の活用事例として、保守・運用の委託契約・守秘契約の条項モデルを紹介する。



このほか、契約で特定されていない場合でも解釈の資料として活用できる。たとえば、事故発生時の責任について契約関係にある場合は保護しなければならないが、相手を加害した場合は付随義務の判断として、社会通念に照らして、債務者の責めに帰することができない場合は免責されるため、この「社会通念に照らして」のところで、ISO/IEC 27017 が斟酌されるのである。

法律関係にない者同士の場合、たとえば、自社で顧客の個人データをクラウドに入れて、クラウドサービスプロバイダ側が漏えいさせてしまった場合、顧客と自社間では契約関係にありながらも、個人情報保護法上の義務を問われる可能性がある。その場合、自社はプロバイダに対し適切な問いかけを行っていたか、適切な情報、判断をもって委託していたかが立証でき、また、漏えいした側のプロバイダは ISO/IEC 27017 をベースとした ISMS クラウドセキュリティ認証基準に準拠して、ベストプラクティクスを講じていた、といえるようになる。ただし、認証をとっていたから責任が免除される、という解釈はない。しかし、認証を使って立証することができる。逆に認証がなかったら、その立証は困難なものとなることが予想される。



このようにしっかりとしたリスクマネジメントに基づく ISMS クラウドセキュリティ認証の取得・維持は、法的リスクを可視化することに役立つことから、ぜひこの認証のもつ意義を理解して、活用してもらいたい。