2014.08

第１９２回　月例研究会　（２０１４年７月３日開催）

会員番号 1459　武安真児　（情報セキュリティ監査研究会）

【講演テーマ】クラウドサービス利用のための情報セキュリティマネジメントガイドラインの概要及び改訂について

【講師】経済産業省　商務情報政策局　情報セキュリティ政策室　室長補佐　上坪健治　氏

特定非営利活動法人　日本セキュリティ監査協会（JASA）　事務局長　永宮直史　氏

【日時】2014 年 7 月 3 日（木曜日）18:30～20:20

【場所】機械振興会館　地下 2 階ホール

【講演骨子】:講演者より

本年3月、経済産業省では「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を改訂しました。

新ガイドラインは、JIS Q 27002:2006（ISO/IEC 27002:27005)における実施の手引をベースに、クラウドサービス利用における情報セキュリティ管理の確立、導入、運用、監視、見直し、維持及び改善のために必要な情報を提供するものです。本講演では、新ガイドラインの趣旨と概要を中心に解説するとともに、改訂によって生じた主要な変更点についても紹介します。

【講演概要】

講演は、経済産業省商務情報政策局情報セキュリティ政策室　室長補佐　上坪健治氏により行われました。

Ⅰ．情報セキュリティマネジメントガイドラインの概要

経済産業省では、2011 年 4 月に「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（以下「旧ガイドライン」という。）を作成しましたが、2014 年 3 月に改訂を行い、2013 年度版として新たに公表しました（以下「新ガイドライン」という。）。

本講演では、新ガイドラインの概要と改訂内容について説明します。

クラウドコンピューティング（以下「クラウド」という。）は、新ガイドラインでは「共有化されたコンピュータリソース（サーバ，ストレージ，アプリケーションなど）について，利用者の要求に応じて適宜、適切に配分し，ネットワークを通じて提供することを可能とする情報処理形態」と定義しています。

また、クラウドは、世界各地にあるコンピュータ群を仮想化等の先端技術で巨大な1つのコンピュータとして扱えるようにしたもので、提供されるリソースにより、SaaS、PaaS、IaaS に分類されます。

新旧ともにクラウドセキュリティガイドラインは、システム環境が従来のオンプレミス環境からクラウドサービス利用へ急速に変化する中で、必要とされる情報セキュリティ分野の規範として、ISO 27001 や ISO 27002 を利用しつつ、クラウドサービスを利用する上で必要な部分を対応させるために、新たに規定したものとして位置づけられます。

クラウドの安全指針策定と国際標準化の流れを見てみますと、国際規格である ISO/IEC 27002:2005 から日本の規格の JIS Q 27002:2006 が策定され、次に、この JIS Q 27002:2006 をベースに 2011 年 4 月に旧ガイドラインが作成され、さらに、2014 年 3 月に環境変化に対応した改訂版として新ガイドラインが作成されました。

今回、新ガイドラインへの改訂と同時に、「クラウドセキュリティガイドライン活用ガイドブック」（以下「活用ガイドブック」という。）を新たに作成しましたが、この活用ガイドブックでは、具体的な利用シーンに応じたガイドラインの解説を行っています。

また、旧ガイドラインは、ISO/IEC の情報セキュリティに関する専門部会（JTC1/SC27/WG）に提案されていましたが、この専門部会で日本の提案が基礎となったクラウドセキュリティの標準化が行われつつあり、ISO/IEC

27017:2015 として、2015 年に発行される予定になっています。

クラウドを利用する上では、クラウド特有のリスクがあり、そのリスクへの対応が必要となりますが、クラウド事業者と利用者間で情報セキュリティポリシーの不整合が存在し、データ管理のレベルが異なることなどにより、不正なデータ取得によるウイルス感染や、適切なアクセス権の設定不能、また、ライフサイクル管理が困難になるといったリスクが発生します。

さらに、クラウドを利用すると、通常利用者がハードウェアの保有、管理、運用といった自社で行ってきた業務を外注することになるため、物理的なガバナンスの確保が難しくなるとともに、社内にスキルが蓄積出来なくなり、システムの構築・運用・管理に関するリテラシーが低下するという問題が起こります。

これらの利用者の不安を防ぐには、懸念事項は何かをしっかりと分析し、原因に対して管理策を講じることが必要になります。

クラウドを利用する上で発生するリスクを回避するために、クラウド事業者とクラウド利用者がお互いに協力・連携して情報セキュリティ対策を実施し、安全・安心なクラウドサービス利用環境を保証するための枠組みを構築することが必要となります。このようなリスクへの対応が、クラウドセキュリティガイドラインの目的です。

Ⅱ. 旧ガイドラインの策定

旧ガイドラインの策定では、アンケートを実施して情報セキュリティ対策のニーズの調査を行いました。実施したアンケートの中では、クラウド事業者による情報セキュリティ対策の第三者評価及び情報セキュリティマネジメントシステムの国際基準への適合性評価の要望が多いことが分かりました。

また、クラウドセキュリティガイドライン（初版）が出来た背景としては、クラウドの黎明期の 2008 年からの 3 年間でも多くのインシデントが発生していて、クラウドに対してルールが必要になったこともありました。

そこで、ガイドラインの内容と構成は、JIS Q 27002:2006 の章立てに 1 対 1 に対応させ、クラウド利用者の具体的な対策とクラウド事業者の実施が望まれる事項を分けて記述しました。

具体例をスライド 10 ページにあげていますが、オンプレミスを想定して作成された JIS Q 27002:2006 では、情報システムの「利用」という形態をとるクラウドには、管理策の「実施の手引」をそのまま適用することはできませんので、「クラウド利用者のための実施の手引」、「クラウド事業者の実施が望まれる事項」及び「クラウドサービスの関連事項」の3つに分けて記載しています。

Ⅲ. 新ガイドラインの改訂と活用ガイドブックの作成

新ガイドラインの改訂の理由は、以下のとおりです。

①クラウドを本格的に運用していく過程で、大規模な障害や障害対応過程での情報漏えい等が発生したことにより、リスクが顕在化した。

②事業者の情報開示のあり方を詳細に反映することが必要になった。

③国際的な動向を踏まえることが必要になった。

④抽象的な条文だけでなく、具体的な利用シーンに応じた対策についての解説が欲しいという声があった。

これらの要望等を踏まえ、新ガイドラインと活用ガイドブックを作成しました。

ところで、新ガイドラインとは別に、総務省から「クラウドサービス提供における情報セキュリティ対策ガイドライン～利用者との接点と事業者間連携における実務のポイント～」が今年 4 月に発表されています。何が違うのかよくご質問を受けるので、経済産業省のガイドラインとの違いを説明します。総務省のガイドラインは、クラウド事業者のなかでは SaaS 事業者が多いため、SaaS 提供におけるアプリケーションに関わる領域に特化して、実務の詳細を記述して

いますが、経済産業省のガイドラインは、クラウド利用者と事業者の双方を対象とした内容になっており、SaaS 事業者も含めた汎用性を持っています。

また、「クラウド情報セキュリティ管理基準」が日本セキュリティ監査協会から発表されていますが、こちらは対策技術の実装について、参照する基準が必要になったときに利用するものになっています。

Ⅳ. ガイドライン改訂の4つの背景とポイント

ガイドラインの改訂は、前述の4つの背景により行われました。

(1)大規模な障害や障害対応過程での情報漏えい等が発生したことによるリスクの顕在化

(2)事業者の情報開示のあり方を詳細に反映することの必要性

(3)国際的な動向を踏まえる必要性

(4)具体的な利用シーンと対策に関する解説の要求

これらのそれぞれについて説明します。

1. 顕在化したリスクに関する改訂

改訂を行うにあたって、発生した以下のリスクの事例を参考としました。

①データ消失を伴う障害の発生(ファーストサーバー事件等)

②電源系のトラブルに起因する長期間のサービス停止を伴う障害の発生(Amazon、Microsoft、Salesforce.com のサービスの停止等)

③容量・能力管理に関する障害の発生(Amazon、Microsoft Azure のサービスの停止等)

新ガイドラインは、これらに対応した改訂を行っていて、具体的な変更点は以下のとおりです。

(1)情報のバックアップ(箇条 10.5.1)

バックアップ取得に関する要求事項をさらに明確化しました。

(2)事業継続計画の策定・実施(箇条 14.1.3)

旧ガイドラインでは、利用者・事業者の基準やシステムの冗長化を図る観点が記述されていなかったため、記述を追加しました。

(3)容量・能力の管理(箇条 10.3.1)

旧ガイドラインでは、事業者への要求事項や関連情報が規定していなかったため、新たに記述を追加しました。

2. 事業者の情報開示のあり方に関する改訂

事業者の情報開示のあり方については、以下の考え方に基づき改訂しました。

a) 利用者への情報提供について事業者自らが方針を定めて利用者に提示し，利用者は提示された方針及び方針に基づき提供された情報によってクラウドサービス利用に係るリスクを評価する。

b) クラウド事業者は，クラウド利用者との合意に基づき情報を開示する。

c) クラウド利用者には，クラウド事業者から情報を得た範囲で自らの責任においてリスクアセスメントを行い，対応や対策を決定する責任がある。

具体的な変更点は以下のとおりです。

(1)操作手順書(箇条 10.1.1)

クラウド事業者に情報提供に関する方針を定め利用者に提供することを求めるとともに、クラウド利用者が管理をクラウド事業者に外注するからといって丸投げにするのではなく、クラウド事業者の情報提供方針を確認することが

望ましいとしました。

（2）第三者によるサービスの変更管理（箇条 10.2. 3）

クラウド事業者は、情報セキュリティに影響する可能性がある第三者サービス提供に変更があった場合は、通知の方針を定めて、新たに事例が設けられた通知事項についてクラウド利用者に通知することが望ましいとするとともに、クラウド利用者も変更管理プロセスに基づき必要な対応を実施することが望ましいとしました。

（3）責任及び手順（箇条 13.2.1）

責任と手順についても改訂が行われ、事業者が情報提供の方針を定めてクラウド利用者に提示することを求めています。

3. 国際的な動向

前述のとおり、クラウドセキュリティガイドラインを国際標準化する作業が行われていますが、2015 年に ISO/IEC 27017 が発行されると、新ガイドラインはそれに合わせて役割を終える予定です。

（1）分類の指針（箇条 7.2.1）

データの分類項目の例を明確化しました。事業者だけでなく、利用者もきちんと資産に対するチェックを行うことが示されています。クラウドサービスは事業者と利用者が相互に協調することが必要であることの一例です。

（2）モバイルコードの管理策（箇条 10.4.2）

事業者は方針を定め、クラウド利用者に提示し、方針に対する協力を求めるとともに、クラウド利用者も悪意のあるコードに関する事項について、クラウド事業者の情報提供方針を確認することが期待されています。

（3）ネットワーク管理策（箇条 10.6.1）

通信傍受が話題になっていますが、利用者と事業者ともに暗号化やアクセス制御等に注意することを記述しています。

（4）ネットワーク領域分割（箇条 11.4.5）

仮想化を行う場合、ネットワークの仮想環境の分離があいまいであると問題が発生するため、基盤についての管理を利用者も事業者もきちんと行ってほしいということを新規に記述していて、さらに、クラウド利用者からネットワークを分離する機能の使用について、必要に応じて情報を要求するケースについて記述しています。

4. 活用ガイドブックの作成

活用ガイドブックは、以下の 5 部構成になっています。

1. はじめに　　2. クラウドセキュリティとは　　3. クラウドサービスにおけるリスク

4. クラウド利用者のためのガイドライン活用　　5. クラウド事業者のためのガイドライン活用

ガイドブックは、ガイドラインを読む前に読むと、ガイドラインを理解しやすいと思われます。とくに「3. クラウドサービスにおけるリスク」では、クラウドサービスにおける様々なリスクについて解説されていて、これとガイドラインの参考となる項番が対応付けられているため、ガイドラインの重点項目がわかる構成になっています。

また巻末に、付録として契約書等の書式のサンプルを用意しました。実務において有益な内容になっているかと思いますので、ぜひご参照ください。

Ⅴ. 今後の動向

1. クラウド情報セキュリティ監査制度

クラウドセキュリティをきちんとセキュリティ基準に基づいて行っていることを外部に示して信頼性を向上するために

は、本来外部の専門家の確認を受けることが望ましいことです。しかし、外部の専門家による監査は一般にコストも時間もかかるので内部監査をきちんと行い、さらに当該内部監査について信頼性があることを確認できれば、コストや時間をそれほどかけずに信頼性を向上することができます。この内部監査の信頼性を確認する制度が、クラウドセキュリティ情報監査制度で、予定では今年度中に実施できる見込みです。

2. クラウド情報セキュリティの国際標準化

国際規格である ISO/IEC 27017 の標準化は、2011 年 5 月から行っていて、それと並行して、ISO/IEC27036-4: 供給者関係の情報セキュリティの標準化に向けた議論も行っています。

また、クラウドセキュリティ監査制度に関する議論や、クラウドリスクの管理フレームワークに関する議論も行っています。

これらは、2014 年 10 月をもって基本的な議論が収束し、骨子が決まる状況であると聞いています。

今後はこれらの周辺の部分についての議論を行い、来年秋ごろに正式な ISO/IEC 27017 のスタートが出来ればという状況になってきています。

Ⅵ. 資料

ガイドライン及び活用ガイドブックは、以下のホームページに掲載されています。

・新ガイドライン及び活用ガイドブックの原文

http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html

・旧ガイドラインの原文

http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

Ⅶ. 質疑

質疑では、特定非営利活動法人　日本セキュリティ監査協会（JASA）事務局長　永宮直史氏と経済産業省商務情報政策局情報セキュリティ政策室　室長補佐　上坪健治氏のお二人に回答していただきました。

最初に、すでに参加者から事前に受け付けた質問について、回答が行われました。

質問1：クラウド利用者が安心してクラウドサービスを利用するために、クラウド事業者が必要な情報を利用者に開示しなければならないが、そのための制度面の方策はありますか？

回答1：クラウド情報セキュリティの認証制度までは話が進んでいませんが、ISO/IEC 27017 が発行されるまでには議論をしなければならないと言われています。事業者が内部監査を行う時の管理基準は作りましたが、監査をして欲しいとの要望がありますので、まず監査制度を立ち上げようとしています。

質問2：クラウドサービスのプライバシー保護に配慮したデータの利活用・流通はどのように考えればよいでしょうか？

回答2：新ガイドラインは、プライバシー保護については範囲外としています。セキュリティとプライバシー保護には密接な関係がありますが、本来、別のものです。クラウドにおける PII（個人の識別）は、現在並行して ISO/IEC 27018 で検討されていて、これに基づく対策が本来、必要になるものと思われます。

質問3：従来の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」の利用・適用実績はどれくらいありますか？

回答3：実績については調査をしていません。ただし、情報セキュリティに関心の高い大手の企業では、事業者に対してチェックリストを作成して、履行状況を確認したと聞いています。

質問4：本来、クラウド利用者にとってのクラウドの価値はその利用の手軽さにあると思われますが、ガイドラインが求めているものは手軽さに反するという批判は無いでしょうか？

回答4：手軽さに反するという批判は無いと思いますが、「厳格に守って下さい」では厳し過ぎると言われることは理解できます。

JASA のホームページに「クラウド情報セキュリティ管理基準」を掲載していますが、この中の「基本言明要件」が、中小事業者が利用できるセキュリティ基準になりますので、管理策の判断基準としてください。

なお一言申し上げておきたいのが、新ガイドラインは、法令ではありませんので、それ自体には罰則はありませんが、会社経営者が負う「善管注意義務」を測る尺度になり得るということです。事業者・利用者いずれの立場でクラウドを利用するにせよ、システムの運用姿勢に問題があり、損害賠償等の問題が発生した場合、会社経営者の過失の判断基準の一つとして新ガイドラインが用いられ得るということはご認識ください。

質問5：「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」で触れられている範囲内でのセキュリティ事故はどのようなものがありましたか？

回答5：新ガイドラインは、利用者側の目線で書かれているので、利用者がどのような事故が起きているかを把握することは難しいと思われます。事業者側から聞いた話では、クラウドの管理者権限の乗っ取りと利用者の安易なサーバの消去がセキュリティ上のリスクになるということです。

質問6：小企業の場合は、自社で情報システムを管理できないためにクラウドサービスを利用するのですが、クラウドを利用する場合、サービス事業者に任すことができず、利用者自身で実施しなければならない事項があると思われます。何を実施しなければならないかについての一般的な例がありますか？

回答6：クラウドは、それぞれサービスが異なるため、クラウドに一般的なものというのはありません。自社で対応できない場合には、そのサービスを提供してくれる事業者を選定して依頼する必要があります。

質問7：クラウドサービスを利用する場合、監視のためのログ取得とチェックについて、利用者が行わなければならない部分についての基準はありますか？

回答7：クラウドは、サービス内容が事業者によって異なり、同じ事業者でも異なるサービスを提供しているため、基準となるものはありません。自分が出来ることに合ったクラウド・サービスを選択してください。

質問8：クラウドの事業者やサービスを検討して選択することも、利用者にとっては技術力と工数が必要になると考えられますが、第三者の立場で選択の相談に乗ってくれる機関は無いでしょうか？

回答8：民間の SI 事業者さんがこういったサービスを行っているところがあります。コンサルタントといえばコンサルタントですが、よく分かっているので、心配であればそういうところを利用することも考えられます。

最後に会場から、以下の質問がありました。

質問:いわゆる自称クラウド事業者に関してそのようなあまり信頼できない事業者への対応はどうすればよいでしょう？

回答:そのような自称クラウド事業者を排除できるかは疑問です。クラウドは、もともと設備から出た概念ではなく、サービスから出た概念ですので、「御社はクラウドでは無い」と明確に言うことができません。しかし、透明性は必要で、例えば、日本では食品については食品衛生管理制度があります。おいしいかどうかはわかりませんが食中毒を起こさないことの線引きが明確にできます。今後、クラウドサービスが公共サービスになって行くと考えられますが、最低限の品質を確保するためにも、監査制度を現在、作っています。

質問:クラウド・イン・クラウドの問題で、ユーザからは表に出ているクラウド事業者しか見えないため、その後ろにいるクラウド事業者が見えませんが、利用者から見て安心できないのではないでしょうか？

回答:クラウド事業者は、後ろのクラウド事業者についても安全性を明確にしなければなりませんが、それが出来ない場合には、後ろの事業者に問題が起きた場合、その全ての責任を表に出ているクラウド事業者が取る必要があります。

以上

＜目次＞