Vol.2013-EIP-59 No.1
2013/2/15

クラウドサービス利用における第三者認証制度の考察

佐藤 栄城[†1]、原田 要之助[†1]

近年、パブリッククラウドサービスが普及しており、ユーザ企業（以下、ユーザという）は自社でハードウェアリソースなどを管理することなく様々な情報システムを利用することが可能となっている。しかし、多くのユーザは自社管理下と比べて情報セキュリティの脅威をパブリッククラウドサービスよりも高く感じているのが現状である。そのため、パブリッククラウドサービスを受けるときに、事業者を選定する上で ISMS や P マークなどの第三者認証取得の有無を参考とすることが多い。これらの認証制度はユーザが期待する情報セキュリティを必ずしも保証するものではなく、ユーザの期待と実際の保証との間にギャップが生じていると考えられる。これらを示す例として、両認証を取得していたファーストサーバ社(FS 社)が引き起こしたデータ滅失・漏えい事故について考察する。
本稿においては、FS 社の事故を参考に ISMS や P マークなどに見られる第三者認証制度や保証サービスなどの特徴を比較し、その問題点について考察した。また、クラウドサービスなどの第三者認証制度や保証サービスに求められているものと現実とのギャップを説明するモデルを考察した。

A study on the problem of use Third-party certification in case of cloud services

EIKI SATO[†1]　YONOSUKE HARADA[†1]

Recently, public cloud services have become popular. Business users can choose various information services without managing hardware resources on-premises, but the other hand, higher security threats compare with in-house systems are identified and recognized. Therefore, user entity tends to refer the presence of third parties certificates, such as the Privacy Mark (P-mark) of Japan or ISO/IEC 27001(ISMS) Certification, for selection of a cloud service provider. There is a gap between the user's expectations and the actual warranty coverage, for instance, guarantee of system safety is not considered in certification systems/process. The user's data loss and leakage case by First Server Corporation who has certified both certifications is studied as a case.
In this paper, the features and problems in Third-party certifications as well as similar assurance service, information disclosure are summarized and compared. A model is proposed to explain gaps with actual coverage and the required elements for certification in cloud services.

1. はじめに

(1) クラウドサービスに対するユーザの意識の現状

クラウドサービスは、一般的にハードウェアを自社で持たないことによるコスト削減や運用の容易さといったメリットにより関心を集めており[1]、実際に導入する企業も増加している。一方で、利用を阻害する要因として、主にデータを外部に置くことへの心理的な抵抗が挙げられている[2]。服部は、2010 年に組織のセキュリティ担当者を対象に行った調査[3]において、自組織管理下とクラウドサービスにおいて情報セキュリティ上の脅威をどちらが強く感じるかについて比較した。この結果を図 1-1 に示す。図 1-1 では、クラウドの方に脅威を感じるユーザの割合が多いことがわかる。

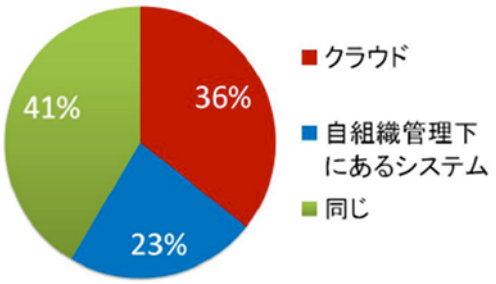

図 1-1 2010 年の脅威の比較(N=311) [4]

情報セキュリティ大学院大学では、2012 年にも同様の調査を実施した。これを図 1-2 に示す。

図 1-2 は、図 1-1 の 2010 年のデータと大きな違いはなく、クラウドに対する不安は未だ解消されていない状況である。このような不安の背景には、クラウドサービスがシステムを自組織管理下に置くことと比較して、ハードウェア、運用の実態などがユーザから直接見えづらく、クラウド事業者とユーザ間で保有している情報に格差が生じてい

1 情報セキュリティ大学院大学　情報セキュリティ研究科
Institute of Information Security

ることが一因であると考えられる.

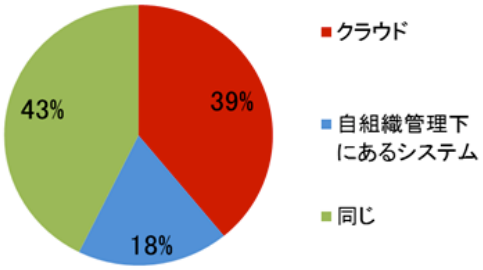

図 1-2 2012 年の脅威の比較(N=328)

(2) クラウドサービスと第三者認証制度

クラウド事業者とユーザ間の情報格差を解消し、クラウド事業者の提供するサービスがユーザの求める要件を満たしているかを確認する手段として、相手先を直接指揮命令し、監査を実施する選択もあるだろう。しかし、クラウドサービスにおいては、クラウド事業者が多数のユーザを抱えているため、ユーザ個別の監査を受け入れることは、監査受け入れにかかわる費用・所要期間の問題により現実的ではない。ユーザ側としても、クラウドサービス利用によるコスト削減のメリットが直接監査により生ずるコスト増で相殺されることは望ましいことではない。そのため、クラウド事業者のセキュリティ対策の確認方法として、公的または中立的な機関による第三者認証の取得を挙げているユーザが多い[1]。栗田・樋口も、このような売り手と買い手で保有する情報に格差がある「情報の非対称」が生じている状態を解消する手段として、クラウド事業者による第三者認証の取得を挙げている[4]。

また、第三者認証の中では、ISMS 適合性評価制度(以下、ISMS 認証制度という)やプライバシーマーク認証制度(以下、P マーク認証という)の認証取得を求めているユーザが多いことがわかっている。これを図 1-3 に示す[3]。

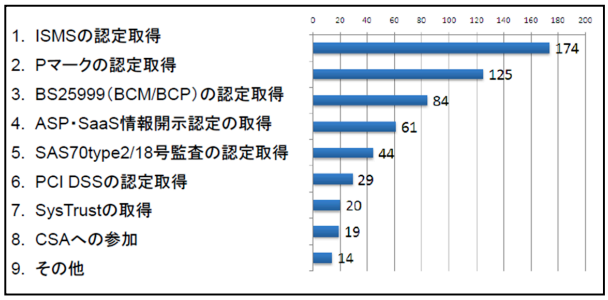

図 1-3 クラウド事業者に備えていて欲しい第三者認証 (N=316) [3]

クラウド事業者がこれらの第三者認証を取得していれば、一定度合のセキュリティ対策が実施されていることや、万一事故等が発生した際には、認証機関により適切な措置が実施されることを期待していたユーザも少なくないだろう。しかし、2012 年 6 月 20 日に発生したファーストサーバ社(以下、FS 社という)が引き起こしたユーザデータ滅失・漏えいは、ISMS および P マーク認証を取得している事業者の事故であったことから、クラウドサービスと第三者認証制度、および両者の関係について整理し、その問題点を示すことが喫緊の課題であると言えるだろう。

2. FS 社の事故と ISMS・P マークの問題

2.1 会社概要

FS 社は 1996 年に設立され、2004 年に Yahoo JAPAN などを運営するヤフー株式会社のグループ会社となった。主な事業はレンタルサーバサービスであり、同じくヤフー株式会社傘下である IDC フロンティアのデータセンタ設備を利用した高速・大容量のバックボーンネットワークを利用している。また、2012 年現在で約 50,000 ユーザがサービスを利用しており、うち 8 割が法人ユーザである。さらに、ISMS 認証や P マーク認証の取得、SLA(品質保証制度)の導入を行っており、自社のサービスが高品質であることをアピールしている。

2.2 データ滅失事故の概要

2012 年 6 月 20 日 17 時頃、メールシステム障害対応のための FS 社の担当者がメンテナンス作業を行ったところ、担当者が独自に作成したプログラムに不具合があり、「プログラムの適用対象外であった HDD 内に格納されていた」約 5,600 ユーザのデータが滅失した。当該作業は、通常定められているメンテナンス作業と異なる手順で行われていたという。なお、事故発生時の作業担当者 A は、10 年もの間マニュアルで定められていない独自の方式でメンテナンス作業を行っていたが、上長はこれを黙認していたと報告されている[8]。また、FS 社がバックアップと呼んでいるものは、同じ筐体内にあるセカンダリ HDD のコピーデータを指しており、テープなどの外部媒体に保管されているものではない。

表 2- 1 事故発生時の経緯 ※[8]をもとに作成

	通常時の手順	事故発生時の手順
①	社内マニュアルに基づき構成された更新プログラムを検証サーバに適用する。	社内マニュアルを使わず、過去に担当者 A が自ら作成したプログラムを利用した独自の更新プログラムを適用した。
②	検証結果に問題がないことを確認した後、上長に対し本番サーバ群への作業許可を申請し、承認を得る。	上長は会議で不在だったため、許可を得られなかったため、担当者の判断で作業を続行した。
③	「配布システム」を利用しての一部の本番サーバ群下のハードディスク(HDD)に対し更新プログラムの適用を行う。	「配布システム」を利用せず独自の方式でセカンダリ含む全ての対象 HDD に対しプログラムの適用を行った。

④	問題がなければ、対象となる残りの本番サーバ群の各サーバのプライマリ HDD 全てに対し更新プログラムの適用を行う。	更新プログラムの適用対象外であったサーバのデータがバックアップ(セカンダリ HDD のデータ)を含めて全て滅失した。
⑤	毎日午前 6 時 30 分に本番サーバ群のプライマリ HDD のデータがセカンダリ HDD に自動でコピーされる。	

2.3 データ漏えい事故の概要

FS 社は、データ滅失事故発生後、ユーザからの要望により滅失したデータの復元作業を行った。しかし、FS 社が提供した復元データには他のユーザのデータが混在しており当該情報が漏えいした。

漏えいに至った要因として、FS 社がデータ滅失事故を組織として想定していなかったことが挙げられる。オープンソースソフトウェアを利用したデータ復元作業の実施を決定したが、当該ソフトを利用することによる漏えいのリスクは業界内で比較的一般的に知られている事項であった[8]のにもかかわらず、これを認識していなかった。

2.4 FS 社の事故発生後の対応

事故発生後の FS の対応について、表 2-2 の通りまとめた。6 月 20 日の 17 時 50 分にサービス利用不可であることを認識した後、同日 20 時 00 分にユーザデータ復元プログラムの検証を開始していたことから、この時点でユーザデータが滅失していることを認識していたと考えられる。しかし、実際にデータの滅失とサーバの初期化を発表したのは 6 月 21 日 3 時 30 分であり、滅失の認識から公表までは時間差がある。基本サービスの再開が約 1 日、オプションサービスを含めた全てのサービス再開まで約 2 日であった。サービス再開後も対応状況をウェブサイトに掲載しており、一定度合の説明責任を果たしている点は評価することができる。

表 2-2　事故発生後の対応 ※[8][9]をもとに作成

	日付　(時刻)	FS 社の公表内容[9]	第三者報告書に記載の事実[8]
①	2012/6/20 (17:50)	サービス利用不可であることを確認、原因調査を開始 (※データ滅失発生)	
②	2012/6/20 (20:00)		ユーザデータ復元プログラムの検証を実施
③	2012/6/20 (22:00)	サポートページにて情報提供を開始	
④	2012/6/21 (3:30)	ユーザデータが滅失していることを発表、サーバの初期化と一部サービスのデータ復旧作業実施を発表	
⑤	2012/6/21 (9:00)		復元したファイルの提供開始 (※データ漏えい発生)
⑥	2012/6/21 (23:00)	基本サービスの再開を完了	
⑦	2012/6/22 (18:00)	オプションサービスを含めた全てのサービスの再開を完了	
⑧	2012/6/22 (21:00)		復元データに他ユーザのデータが混在していることを確認したため、提供を中止
⑨	2012/6/23	お詫びとお知らせを掲載	
⑩	2012/6/25	中間報告と FAQ を掲載	
⑪	2012/6/28	第三者委員会設置について公開	
⑫	2012/7/2	情報漏えいについての報告を公開	
⑬	2012/7/13	「損害賠償のご案内」の発送を開始	
⑭	2012/7/31	第三者調査委員会による調査報告書を受領・公開	
⑮	2012/8/10	事故の再発防止策の実施計画を公開	

2.5 FS 社の事故発生後の対応

表 2-2 上の「損害賠償のご案内」は、FS 社のサービス利用約款[10]に準じ、「これまでにユーザが支払った利用料金の上限」を損賠賠償として支払うものであった。「結果的損害、付随的損害、逸失利益等の間接損害」については、約款上で免責事項として挙げられており、賠償額に含まれていない。

このような、損害賠償額責任に制限を設ける規定の根拠となる判例として、日本電信電話公社（現 NTT）世田谷ケーブル火災事件[11]が挙げられる。原告（地元商店の店主ら）が、電話の不通により営業上の損害を受けたとして被告（日本電信電話公社）に総額 4700 万円の損害賠償を請求した。しかし、東京高裁は、「電気通信サービスの不提供から生じるすべての損害を予測して料金に反映させることは困難である」、「通信サービスの不提供から直接・間接に生じる損害は多大となるので電電公社に過大な負担を強いる恐れがある」などの点を指摘し、公衆電気通信法 109 条が電話使用料金を基準に損害賠償額の上限を設ける規定は有効であると判断し、原告の請求を棄却した。

なお、先述した免責事項は「故意または重過失が存在する場合」、「契約者が消費者契約法上の消費者に該当する場合」には適用しない旨も明記されているものの、第三者委員会による事故調査報告書[8]では、事故について「故意と

同視できるほど悪質な過失(重過失)ではない」としており、免責事項に該当しないと解釈されている。

以上のことから、ユーザが間接損害を含めた賠償を受けるには、FS 社の事故が重過失であることをユーザ自らが立証しなければならず、非常に困難であると言える。

2.6 再発防止策

FS 社は、事故の再発防止策として、下記事項を挙げている。

① 開発・運用プロセスの見直し
② 牽制（開発・運用）を含めた体制の確立
③ システム変更業務の運用移管と分掌整理
④ 2 次バックアップの取得

また、データ漏えい事故の再発防止策として、下記事項を挙げている。

① データ漏洩事故の前提となった、データ滅失事故の再発防止策の実施
② データ滅失時の対応マニュアル整備
③ リスクマネジメントに関する組織の設置

第三者調査委員会は、再発防止策について「これらの予防策が実施され、機能した場合には今回発生した事故を防ぐことができる」とし、「一般的なレンタルサーバ業者の水準に照らし合わせて適切である」と評価している[8]。

2.7 まとめと問題点

データ滅失・漏えい事故の復旧や再発防止策、(限定的な)損害賠償の支払いなどの一連の対応が行われ、事故は収束したとも解釈できる。しかし、ユーザがクラウドサービスを利用する上での不安は解消されているわけではない。特に、FS 社は ISMS および P マークの両認証を取得し、本来はこのような事故を防止する体制の構築を期待されていることから、第三者認証制度に何らかの問題があると考えられる。

3. ISMS・P マーク認証制度と事件への対応

本章では、FS 社の事故について、同社が取得していた ISMS・P マーク認証制度の観点から、要求事項上問題となると想定される下記①～③の事項について考察する。あわせて、事故後の認証機関の対応の問題点についても検討する。

①組織のマネジメントシステムの問題

担当者が 10 年もの間マニュアルで定められていない独自の方式でメンテナンス作業を行っていたことを、上長が黙認していた。

②管理策の内容の問題

FS 社がバックアップと称しているものは、同じ筐体内にあるセカンダリ HDD のコピーデータを指しており、テープなどの外部媒体に保管されているものではなかった。

③データ復旧手順の不備

データ復旧のための手順そのものが存在していなかった。

3.1 ISMS 認証制度

ISMS 認証制度は、日本工業規格である JIS Q 27001（情報セキュリティマネジメントシステムの要求事項）に適合している組織を認証する制度である。認証を受ける組織は、特定した「情報資産」へのリスク評価を行い、必要なセキュリティコントロールを実施する。また、PDCA サイクルの採用により、運用管理された情報セキュリティを生み出す一連のプロセスの改善を継続的に行う[12]。

(3) 認証機関の対応

事故発生から一週間後、認証機関のウェブサイト上にて事実関係の調査を行う旨が発表された[13]。その後、約 2 か月後の第三者調査報告書が公表された後の 8 月 16 日に、FS 社の ISMS 認証資格が「マネジメントシステムの不適合の是正処置とその有効性が確認できるまで」一時停止された[14]。その後、10 月 12 日に「臨時審査の結果、再発予防策とその有効性の確認ができた」として、一時停止の解除が発表されている[15]。

ISMS 認証制度においては、ISO9001 認証取得事業者の不祥事発生時の対応手順[2]を適用したものと考えられる。

(4) 制度の問題点

システムのバックアップやデータ復旧手順については要求事項に規定されているものの情報そのものなのか媒体に対するものかが不明である。また、組織が特定した個人情報（資産）に対するリスク評価とそれを低減する管理策の有効性については、審査員が判断することになる。例えば、データのバックアップについて「ユーザデータについてはユーザ側にバックアップを依頼しており、自社側のバックアップはシステム保全用である」と説明すれば、FS 社が実施していた方式は管理策として十分であり、ISMS の要求事項上としての問題はないと判断される。そのため、ユーザが事業者を選定するときには、ISMS 認証を受けているので、クラウドサービスに要求されている管理策がすべて実施され、適切なレベルが達成されていると考えてしまう。しかし、ISMS 制度としては、ユーザが期待することの何らの保証もしていない。また、管理策実施の有無を記した「適用宣言書」はセキュリティの観点から非公開が原則であり、ユーザが管理策について確認することができない。

以上のことから、クラウド事業者が ISMS 認証を取得し

2 詳細手順については[16]を参照

ていることを判断材料として、情報セキュリティのレベルを判断することには限界があると言える。

3.2 P マーク認証制度

P マーク認証制度は、日本工業規格である JIS Q 15001（個人情報保護マネジメントシステムの要求事項[17]）に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定し、当該規格へ適合していることを示すマークの使用を認める制度である。JIPDEC は、P マーク制度の認定を受けることで、平成 17 年 4 月 1 日に施行された「民間企業の個人情報の保護に関する法律（個人情報保護法）」に適合していることをアピールできるとしている[18]。

(1) 認証機関の対応

通常、認証の取消または一時停止が行われた場合は JIPDEC のウェブサイトにて企業名が公表されるが、当該部分に FS 社が記載されることはなく、11 月 20 日に本件事故に対する注意喚起[19]および審議結果[20]（漏えい事故について注意を実施）の公開が行わるまでは、審議の経過などについて何ら情報公開が行われていなかった。審議結果の内容と問題点については、次項にて述べる。

(2) 制度の問題点

保証対象が個人情報保護を目的とした「マネジメントシステム」であるため、ISMS 認証と同様の問題が存在すると考えられる。

さらに、クラウドサービス分野における P マーク認証制度の問題の一つに、「JIS　Q15001 の要求事項の適用範囲である事業の用に供する個人情報の解釈」がある。経済産業省が公表している個人情報の保護に関する法律についてのガイドライン[21]では、レンタルサーバ内の情報は「事業の用に供しない個人情報」と解釈することが可能であり、P マークのマネジメントシステムの適用範囲外であると言える。このことから、佐藤・原田は、「サービスの性質上、サーバ内に個人情報が保管されることは容易に推定可能であることから、先述した解釈が妥当であるかについては疑問が生じる」と批判している[21]。

(3) 過去事例と FS 社への対応

FS 社の事故に対する措置について、過去事例から考察を行う。判断基準によれば、「事業者としての故意」の事故における欠格レベル 10（取消）、不可抗力による事故の場合の欠格レベル 0（措置なし）以外は、各事故の類型・原因により欠格レベルの判断が行われることとなる。しかし、このレベルは抽象的であり、第三者から見て客観的とは言えない。

表 3-1 は、過去の代表的な事例と措置についてまとめたものである。2007 年に発生した大日本印刷の委託先社員による情報窃取は、約 863 万件の個人情報漏えいが発生する大規模なものであった。しかし、当時は表 3-2 で挙げた一時停止の措置が規定されておらず、勧告措置にとどまった[20]。三菱電機インフォメーションシステム（以下、MDIS という）は、自社が提供している図書館情報システムのパッケージソフトウェアに、他の図書館のセンシティブ情報が残っていたまま提供したことにより、漏えいが発生した[24]。千代田興産は、MDIS のパートナー企業であり、同システムの運用を行っていたが、パスワードの管理不備により利用者情報を外部から参照可能となっていた[24]。ともに過失（管理不備）とされ、P マーク付与の一時停止が行われた。

表 3-1　P マークの過去の措置事例

発生年月	事例	原因	規模	措置
2007 年 2 月	大日本印刷	過失（委託先の社員による情報窃取）	約 863 万件（漏えい）	勧告 ※当時の判断基準においては取消に次ぐ措置
2010 年 9 月	三菱電機インフォメーションシステムズ（MDIS）・千代田興産	過失（管理不備）	約 3,000 件（漏えい）	一時停止
2012 年 6 月	ファーストサーバ（FS 社）	過失（管理不備）	約 5,600 件（滅失） 約 2,300 件（漏えい）	滅失：措置なし 漏えい：注意

最終的に、認証機関が公開した注意喚起[19]と審議結果[20]においては、佐藤・原田の指摘と同じ解釈を行い、データ滅失については「個人情報の取り扱いに該当しない」として「措置なし」であった。しかし、データ漏えいについては、「復旧作業に着手した時点で保存されている情報に関わりないとは言えず、個人情報を取り扱う地位にあった」と指摘し、「他の契約者にアクセス可能な状態になっていたことは、個人情報保護マネジメントシステムが十分に機能しているとは言えない」とし、FS 社に責任があるとした一方で、「個人情報の一部が散在するかたちで混入しただけでは直ちに本人に被害が生じるわけではなく、二次被害の可能性もなく、個人情報の流出としては極めて軽微な事例であった」と評価し、最終的に「注意措置」相当と判断した。通常、注意措置の場合は情報公開されることはないが、社会的な影響の大きさを考慮した結果、再発防止策の定着度合が確認されるまでの間、審議結果を公開している。

このように、クラウドサービスでユーザが蓄積・保存して利用している個人情報が、クラウド事業者側にとっては、個人情報に該当しないという見解は、クラウド事業者を選定する材料として P マーク認証取得の有無が参考にならないことを示している。ユーザはクラウド事業者選定プロセスを見直す必要があると考えられるが、当該注意喚起につ

いて、事故から半年後にウェブサイトで掲載されているのみであり、十分に周知されているとは言えない。

3.3 ISMS・P マーク認証制度の限界

以上のことから、ISMS・P マークの認証制度はユーザがクラウド事業者を選定する際の材料として利用するには問題があり、図 1-3 で示されているユーザの期待に応える制度設計になっておらず、「期待ギャップ」が生じていると考えられる。もともと、製造物製品と情報システムの認証制度の違いとして、製造物製品は、製品の種類ごとに品質基準が法的または業界により定められていることが多いが、情報システムについては、データとそれらを処理する作業が特定されない限り、対策レベルを具体的に一般化することは困難であり[26]、その基準が定められている分野はごく限られている。そのため、ISMS や P マーク認証の取得が、クラウドサービスにおいて一定以上の品質基準を満たしていることを保証できるわけではない。こうした認識が一般に浸透しているとは必ずしも言えない状況であると考えられる。とくに、クラウドの IaaS においては、事業者はインフラ部分の提供に留まり、ユーザが扱うデータの種別を事業者は認知できないことから、ユーザは事業者が提供するサービスレベルに同意した上で利用していると主張することも可能である。一方、クラウドの ASP や SaaS の場合、事業者側がアプリケーションを提供している以上、事業者が提供するサービスに入力される情報の種別については一定度合認識しているとみることもできる。しかしながら、いずれの場合においても、利用者に均一の規約(約款)によりサービスを提供するクラウドサービスの性質上、どのような情報セキュリティ対策を行うのかは最終的に事業者側の判断であり、個別のユーザの期待に応じるとは考えにくい。

しかしながら、制度への信用失墜を防ぐために、P マークについては欠格レベルの判断基準をより客観的で具体的なものに改訂することや、第三者機関による認定機関の監査等が任意に実施できるようにするなど、早急の改善が必要であるのではないであろうか。

4. 他の第三者認証・保証制度

4.1 ITSMS 適合性評価制度

ITSMS 適合性評価制度(以下、ITSMS 認証という)は、日本工業規格である JIS Q 20000 (IT サービスマネジメントシステムの要求事項)に適合している組織の IT サービスを認定する制度である[27]。ISMS 認証制度が、組織の情報資産を対象としているのに対し、ITSMS は IT サービス（全体または一部）の品質マネジメントを対象として認証を行う点が大きな違いである。「サービス継続及び可用性に対する要求事項」をもとに平時および緊急時の管理策を策定するため、ISMS と比較して特に可用性が重視されている。また、ITSMS 上の機密性に対する要求事項に該当する「情報セキュリティ管理」は、ITSMS ユーザーズガイド[27]において「ISMS を要約したものであり、ITSMS の適用範囲が ISMS を構築した範囲に含まれる場合はその仕組みをそのまま使用できる」としており、両規格を併存させることができる。

以上から、ITSMS 認証は、クラウドサービスの可用性の判断材料として利用が考えられるが「どのサービスレベルで合意が成されているか(SLA)」を併せて確認する必要がある。

2012 年 7 月時点の ITSMS 認証取得組織数は 170 弱程度であるが、そのうちクラウド事業者による取得割合は少ない。

4.2 SOC 報告書

公認会計士による委託先企業の内部統制や運用状況を保証する制度の代表的なものとして、SOC 報告書業務が挙げられる。SOC 報告書業務は米国の公認会計士協会(AICPA)により、用いる基準や保証対象、利用目的の違いなどから SOC1・SOC2・SOC3 に分類されている[28]。SOC1 は財務諸表に関係する内部統制が保証対象である。なお、「SAS70type2」および「18 号監査」は現在の SOC1 で用いられている基準の旧規準にあたる。SOC2 は財務諸表関連以外の業務システムのセキュリティ、可用性、処理のインテグリティ、機密保持、プライバシーに関する内部統制を対象とする保証である。しかし、SOC1 と SOC2 の利用は監査目的に制限されている。そのため、企業のウェブサイト上では、「SOC1 報告書を受領した」などの記載に留まり、具体的な保証範囲は明示されない。SOC3 は、SOC2 と同様の保証対象であるが、報告書の記載内容は簡易的なものとなっている。また、利用目的に制限はなく、ウェブサイトに認定シールを表示する形態である。

もともとクラウドサービス向けに策定された制度ではない上、他の認証制度と比較して、監査法人が保証するために、保証取得の費用と準備に時間がかかる。米国では、クラウド事業者が SOC2 を利用しているが、日本においては、SOC1 にとどまっている。

4.3 PCI DSS

PCI DSS は、PCI SSC によって策定された、クレジットカード情報保護を目的としたセキュリティ基準である。実装レベルでの情報セキュティ水準が定められているのが特徴であり、その内容も公開されている[31]。審査は企業規模に応じて、訪問審査、サイトスキャン、自己問診 などが行われる。

日本においてはクレジットカード業界を中心に普及が進んでいるが、制度の目的がクレジットカード情報の保護にあり、クラウドサービス向けに最適化されたものではない。そのため、当該情報を取り扱うようなクラウドサービスを提供する一部事業者を除いて、普及していない。

4.4 BCMS

BCMS 適合性評価制度は、ISO22301 にて規定されている事業継続マネジメントシステムの要求事項に適合している組織を認定する制度である[32]。組織の現状を把握し、策定した事業継続計画の実効性を演習実施により確認し、自然災害やテロなどから組織にとって重要な業務の停止につながるリスクを最小限に抑え、事業継続を行っていくことを目的としている。

図 1-3 の通り、ユーザからの要求は比較的多いが、クラウドサービスを含む IT サービスを対象としたものではない 。クラウド事業者が当該認証を取得していたとしても、ユーザのデータの保全やサービス提供が、事業者の事業継続とどのように関係しているかを正しく確認する必要がある。

4.5 問題点のまとめ

上記のクラウド事業者による取得が想定される第三者認証制度・保証制度について表 4-1 の通りまとめた。

表 4-1　第三者認証制度・保証制度のまとめ

	制度	対象	備考
1	P マーク	個人情報保護マネジメントシステム	
2	ISMS	情報セキュリティマネジメントシステム	ISO27017 でクラウドに対応
3	ITSMS	IT サービスのマネジメントシステム	
4	SOC1 旧 SAS70 Type2	企業の財務諸表にかかわる内部統制	報告書の利用は内部統制監査目的に限定
5	SOC2	企業の（財務諸表以外の）情報システム一般の内部統制(限定)	報告書の利用はクラウドの内部統制一般の監査目的に限定
6	SOC3	同上（記載内容は SOC2 と比較して簡易）	マーク表示・マーケティング目的で利用可
7	PCI DSS	カード情報保護を目的とした実装レベルのセキュリティ	
8	BCMS	組織の事業継続マネジメントシステム	

まず、ISMS および P マーク以外の第三者認証制度は、図 1-3 の通り、クラウドサービス向けの認証制度としては広く認知されているとは言えないのが現状である。また、クラウドサービスそのものを認証することを目的としている第三者認証制度は現時点で存在していない。

①保証対象の問題

表 5-1 の各制度は、クラウドサービスを認証することを前提としていない。P マークは第 3 章に述べたような問題点があり、ISMS もマネジメントシステムの基準や対象がクラウドサービスに対応していることを確認しなければならない。SOC 1 に関しては、「企業の財務諸表にかかわる内部統制」が対象であるので、クラウド事業者が SOC1 報告書を受領しているとしても、これと無関係なシステムであれば、クラウドサービスのレベルを保証するものとは言えない。

②クラウドへの適用性の問題

ITSMS は、ASP を対象にしていることから[27]、IaaS など他のサービスモデルに対しても適用が可能である。一方で、ITSMS は可用性に関する要求が主であることや、データの保管場所が分散されているなどのクラウド独自のアーキテクチャへの対応が対象外であり。また、SLA を達成できなかった際のペナルティの有無などは、あくまでサービス提供者と顧客間の合意により決定されるため、事故などにより発生した損失が必ずしも補填されるわけではない。すなわち、サービス利用規約や SLA が、自社の要求水準を満たすものであるかを確認していることが前提となる。SOC2・3 も同様で、言明書の記載内容が確認できることが前提となる。

③取得費用の問題

基準の厳格さに比例して大きくなる問題であると言える。取得費用が高くなれば、それに見合ったインセンティブや、法律などによる強制的な推進がなければ、認証を受けようとする事業者が増加しないことは容易に推定される。実際に、ISMS や P マーク認証制度は、政府調達の要件に入ったことから、認証取得が推進された。

④保証内容非公開の問題

報告書の利用対象者が限定されているため、事業者選定の材料としては用いることができないという問題をいう。例えば、SOC1・2 は、契約関係にない第三者向けには「SOC1 報告書を受領した」という記載にとどまり、詳細な内容は公開されない。しかし、これらにより自社のセキュリティレベルの高さをアピールしようとする組織も少なくない。

5. 期待ギャップを考慮した認証制度の評価

5.1 モデルについて

日本のクラウドサービスにおける第三者認証制度および情報公開制度の現状について、第 5 章までで述べた内容から、下記の通りまとめた。

(1) ISMS や P マークはクラウドサービスのリスクに十分な対応ができていないが、それに代わる第三者認証制度のための規格の策定には時間がかかる。

(2) そのため、本来ユーザはクラウドサービスのリスクを認識した上で、より迅速に対応可能である情報公開制度に基づき公開された内容を参照し、事業者選定を行う必要があるが、情報公開制度そのものの認知度は高くなく、一般に浸透しているとは言えない。

(3) 結果として、ISMS や P マークといった既存の第三者

認証制度に依存しているが、これらは制度運用が硬直化しており、ユーザの期待に十分に応えられているとは言えず、クラウド事業者の事故などにより期待ギャップが表面化しつつある。

以上より、クラウドサービスの第三者認証制度の問題は「新しい第三者認証制度」と「既存の第三者認証制度」の両面から検討する必要があり、特に後者の期待ギャップの解消は喫緊の課題であると言える。そのため、第三者認証制度の持つ効果と利用者の認識・期待の関係を評価する必要があると考え、図 7-1 の評価モデルを提案する。

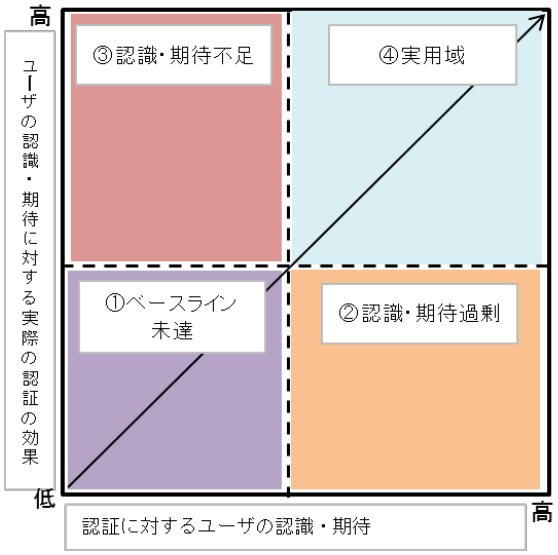

図 5-1 期待ギャップを考慮した第三者認証評価モデル

図 5-1 は、これらの関係をモデル化したものである。図 5-1 の横軸は「認証に対するユーザの認識・期待」を示し、縦軸は「ユーザの認識・期待に対する実際の認証の効果」を示している。前者は「認証制度そのものが広く知られているか」、「何を対象として、どの程度の水準であるか」、「事故発生時のユーザ側の責任の所在」、「事業者選定理由の説明として利用可能か」などについてどのように認識・期待しているかが判断材料となる。後者は、前者に対し、認証制度が実際にどの程度効果があるのかを示しており、両者の交点がその認証の状態を示す位置となる。矢印線は認識・期待と実際の効果が一致している部分を示しており、交点が矢印線から離れているほど「期待ギャップ」が大きい状態を表す。また、図 5-1 中の破線はその分野におけるベースラインを設定する。

図中の位置により、認証制度を下記の①～④の状態に分類した。

①ベースライン未達

ユーザの認識・期待が低く、認証の効果も不足している状態である。

②認識・期待過剰

ユーザの認識・期待が高いが、認証の水準がベースラインに到達していない状態である。

③認識・期待不足

認証水準自体はその分野においてベースライン以上となり得るものであるが、知名度の不足や認証制度に対する不信感がある状態である。

④　実用域

ユーザの認識・期待と認証制度の両方がベースラインを超えていれば、その分野における認証制度として有効に機能しており、実用的と言える状態である。

5.2 評価モデルの適用と考察

前項で挙げたモデルに適用した例を挙げ、考察する。

① ベースライン未達の例

事業者が独自に策定した制度などが該当すると考えられる。策定された水準の根拠が不足しており、社会的な知名度や合意が取れておらず、第三者認証制度としての体裁が不十分である。

② 認識･期待過剰の例

ISMS 認証や P マーク認証は、取得事業者数や知名度により、ユーザからの期待は高いと言える。また、これらの認証制度が情報セキュリティの向上に一定の効果があると社会的に認識されている側面もあると考えられる。しかし、これまで述べてきた「データとそれらを処理する作業の特定」の問題や、P マークの項で挙げた「事業の用に供する個人情報」についての認識クラウドサービス分野の基準として十分ではない。すなわち、認証制度が「何を保証しているのか」についての認識相違の発生が、期待ギャップ発生の一因であることが示唆される。ISMS・P マーク認証が普及してきたことを踏まえ、こうした注意事項などについて事業者やユーザに対し積極的に啓蒙する必要があると言える。

また、ISMS や P マーク認証を取得し、「要求水準を満たしている」と認められているとしても、その管理策のレベルは事業者ごとにまばらであり、認証の効果が一様に定まらない状態である。これは認証制度の性質上避けられない問題であるが、適用宣言書の公開や情報公開制度の利用により、補うことが可能であると考えられる。事業者の管理策の透明性の確保は、認証制度への信頼向上にも役立てると考え、推進していくことも必要ではないだろうか。

③ 認識･期待不足の例

ここに位置する認証制度の課題として、認証取得による事業者側のインセンティブが挙げられる。認証水準を高めれば、認証取得にかかる費用や時間も比例して多くなるため、それに見合った利益を得ることができなければ認証取得する事業者は増加しないであろう。ISMS や P マーク認証

のように、認証取得を入札要件とすることはインセンティブとして効果があると考えられるが、政府などによる関与が得られなければ難しいと考えられる。政府などによる強い関与が得られない場合には、PCI DSS のように適用範囲を限定することや、ITSMS のようにサービスレベルを明確に設定することによって、一定の水準を確保しながら認証取得にかかる費用を低減することが現実的な方法であると考えられる。

④ 実用域の例

クラウドサービス全般を対象とした時に、該当する制度は存在していない。①～③で挙げた問題点を解決することで到達可能となる。しかし、認証制度がこの位置にあるとしても、認証制度の効果を維持するために継続的な取組が必要となる。

一つは、事故を起こした組織への適切な対応である。FS 社のような事故に対し、認証機関による調査・認証停止等の一連の措置、および対応状況について外部への公表が適切に実施されないことは、認証制度への信用が低下し、④の状態から②の状態への悪化を招くことになる。

次に、認証水準と制度運用の定期的な見直しが挙げられる。技術の進化や社会情勢により、リスクが変化し、既存の認証水準や制度運用との間にギャップが発生することは不可避であるが、これらに対応できないことは、認証水準の低下を招き、④の状態から②の状態への悪化を招くことになる。情報システム分野の第三者認証制度においては、先述した「データとそれらを処理する作業の特定」の問題により、クレジットカード情報の保護を目的としている PCI DSS のように適用領域を限定しなければ、認証の効果を一定水準以上とすることは困難である。そのため、ISMS やＰマーク認証制度においては、認証機関・認証取得組織の両者が制度の適切な運用を行うことにより生ずる、一定水準を満たす「実質的な効果」に依存することとなり、事業者を選定する立場のユーザも、その水準を期待していると考えられる。認証取得組織の不祥事や、それに対する不適切な対応は、ユーザの期待を裏切ることにとどまらず、制度の形骸化による実質的効果の低下を招くことになる。

また、一定水準が存在しない分野のベースラインとなるガイドライン等の策定も急務であると考えられる。

6. おわりに

本稿では、クラウドサービスの第三者認証制度の問題点を抽出するため、ＦＳ社のデータ滅失および漏えい事故と、事故に対するＩＳＭＳ・Ｐマーク認証機関の対応の事実についてまとめた。FS 社が取得していた ISMS・P マーク認証の課題から、クラウドサービスの認証としてユーザが事業者の選定に用いるには、情報の非対称性の問題があることを述べた。また、ISMS・P マーク以外の、クラウド事業者による取得が想定される第三者による保証や認定制度においても、最適な制度が存在していないことを述べた。最後に、情報公開制度は、事業者にとって公開の敷居が低く容易に利用できることや、事業者間比較が容易であるなどの特徴と、明確な「保証」がされていないことによる限界について指摘した。さらに、第三者認証制度の評価を評価するためのモデルを提案した。また、モデルの考察を通して、状態ごとの問題点と解決の要素を抽出した。

本研究の今後の課題として、提案したモデルの具体化が挙げられる。

謝辞 本研究にあたり、アドバイスや支援を頂きました情報セキュリティ大学院大学の関係者各位、関係組織の関係者の皆様に、感謝の意を表す.

参考文献

1) IPA「クラウド・コンピューティング社会の基盤に関する研究会報告書」 2010 年 3 月 24 日
2) NRI セキュアテクノロジーズ「企業におけるセキュリティ実勢調査」 2009 年 11 月
3) 服部「クラウドコンピューティング環境におけるインシデントマネジメント手法」、情報セキュリティ大学院、2010 年度修士論文
4) 栗田・樋口「クラウドコンピューティングにおける非対称情報の解消について-第三者認証の活用に向けて-」、情報通信学会誌 Vol.30、NO.1、2012 年
5) NIST Special Publication 800-145,「The NIST Definition of Cloud Computing」September 2011
6) ENISA「Cloud Computing : Benefits, Risks and Recommendations for Information Security」 2009 年 11 月
7) ITmedia「Microsoft の T-Mobile 向けクラウドでユーザーデータ消失」 2009 年 10 月
8) FS 社、「第三者委員会調査報告書(最終版）」、http://support.fsv.jp/urgent/pdf/fs-report.pdf 2012 年 8 月 23 日アクセス
9) FS 社 「6/20 に発生した大規模障害に関するお詫びとお知らせ」 http://support.fsv.jp/urgent/ 2012 年 12 月 12 日アクセス
10) FS 社「レンタルサーバサービス利用規約約款」 2011 年 8 月 18 日版 http://www.fsv.jp/change/pdf/yakkan/rental_server.pdf 2012 年 8 月 15 日アクセス
11) 世田谷ケーブル火災事件（東京高裁 1990 年 7 月 12 日判決） 判例時報 1355 号 3 頁
12) JIPDEC、「ISMS 適合性評価制度概要パンフレット」 http://www.isms.jipdec.or.jp/doc/ismspanf.pdf
13) BSI ジャパン ニュース「「6 月 20 日に発生した大規模障害」の報道があった認証取得組織への対応について」(調査開始) http://www.bsigroup.jp/ja-jp/assessmentandcertification/managementsystem/news/news_source/news20120627/
14) BSI ジャパン ニュース「「6 月 20 日に発生した大規模障害」の報道があった認証取得組織への対応について」(認証一時停止) http://www.bsigroup.jp/ja-jp/assessmentandcertification/managementsystem/news/news_source/20120820news/ 2012 年 8 月 24 日アクセス
15) BSI ジャパン ニュース「「6 月 20 日に発生した大規模障害」の報道があった認証取得組織への対応について」(認

証一時停止の解除)
http://www.bsigroup.jp/ja-jp/assessmentandcertification/managementsystem/news/news_source/20121012news/
16) JAB､組織不祥事への認定･認証機関の対応について(組織不祥事対応検討会 報告書)
http://www.jab.or.jp/files/items/1892/File/08031400-0.pdf
17) 日本規格協会、「JIS Q 15001:2006、個人情報保護マネジメント要求事項」
18) JIPDEC 「プライバシーマーク制度の概要」
http://privacymark.jp/privacy_mark/about/outline_and_purpose.html
19) 日本データ通信協会「データセンター等事業者のサービス利用に関する留意事項等」
http://www.dekyo.or.jp/pmark/sinsei/data/tyuikanki.pdf 2013 年 1 月 4 日アクセス
20) 日本データ通信協会「データセンター等事業者のサービス利用に関する留意事項等」(ファーストサーバ社プライバシーマーク審査結果)
http://www.dekyo.or.jp/pmark/sinsei/data/singiketsuka.pdf 2013 年 1 月 4 日アクセス
21) 経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」 平成 21 年 10 月 9 日
22) 佐藤、原田「情報セキュリティ事故発生時における第三者認証機関の対応についての考察」、システム監査学会第 25 回公開シンポジウム
23) JIPDEC「プライバシーマーク制度における欠格事項および判断基準」平成 24 年 4 月 1 日版
24) JIPDEC「個人情報の事故で大日本印刷株式会社に「要請」処分」平成 19 年 3 月 23 日
http://privacymark.jp/news/20070323/HP_dainihonnjikokouhyou070323.pdf
25) 日経コンピュータ「流出した個人情報は約 3000 件、図書館システム問題で MDIS 社長が陳謝」2010 年 11 月 30 日
http://itpro.nikkeibp.co.jp/article/NEWS/20101130/354715/
26) 社会技術研究開発センター「『企業における情報セキュリティの実効性あるガバナンス制度のあり方』研究開発実施終了報告書」 2010 年
27) IPDEC 「ITSMS ユーザーズガイド」
http://www.isms.jipdec.or.jp/itsms/doc/JIP-ITSMS111-10.pdf
28) あずさ監査法人､「受託会社の内部統制に関する保証報告制度 」KPMG AZ Insight, Vol 47, 2011 年 9 月号
29) 新日本有限責任監査法人､「受託業務に係る内部統制の保証報告書」
30) 日本公認会計士協会 「Trust サービス」
http://www.hp.jicpa.or.jp/ippan/trust/pdf/brochure.pdf
31) PCI SSC 、「PCI DSS 要求とセキュリティ評価手順バージョン 2.0」
https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/pci_dss_v2-0.pdf
32) JIPDEC 「BCMS 適合性評価制度」
http://www.isms.jipdec.or.jp/bcms.html