『ASP・SaaSに対する情報セキュリティ監査をふまえた クラウドコンピューティングに対する一考察』

A study on Cloud computing based on information security audit for ASP･SaaS

佐々木志津香、古江健一、鬼松嵩（情報システム監査株式会社）

１．はじめに

近年、ネットワーク上のハードウェア・ソフトウェアをサービスとして利用するクラウドコンピューティング（以下、クラウド）と呼ばれる形態が急速に普及しつつある(1)。米国のNIST（国立標準技術研究所）はクラウドをサービス形態により下記表１の３種類に分類し、定義している(2)。

表１　クラウドサービスの形態

SaaS: Software as a Service	提供されるアプリケーションを利用する形態
PaaS: Platform as a Service	開発環境を含むアプリケーションとプラットフォームを利用する形態
IaaS: Infrastructure as a Service	提供されたコンピューティング資源(情報処理、ストレージ、ネットワーク等)上で、任意のソフトウェアを利用する形態

このうちSaaS は、既に利用されてきたASP（Application Service Provider)と本質的な違いは無いと考えられる(3)ため、本稿では「ASP・SaaS」と記載し、同義語として扱う。クラウドには利便性やコストの低さ、システム開発期間の短縮など様々なメリットがあり、今後の発展が期待されるが、「自社でシステムを持たない」「ネットワークを通じてシステムを利用する」という特性から、セキュリティリスクについて十分考慮する事が必要である。

米国の情報システムコントロール協会が行った調査によると、IT 専門家の45%が「クラウドはメリットよりリスクが大きい」と考えている【１】(4)。また、経済産業省によるアンケート調査では、クラウドを利用する際の懸念として「セキュリティ対策が十分かどうかわからない」との回答が最も多く挙げられている【２】(5)

しかしシステム経費削減のメリットから、クラウドを導入する企業は増加傾向にある。また東日本大震災発生においては、クラウドコンピューティングを活用した、被災者への情報提供サービス（計画停電情報、支援物資情報、被災情報等）、被災企業や被災自治体へのリソースの無料提供等が行われ、ＢＣＰ対策の面からも注目が集ま

り、着実にクラウドの適用が拡がっている。

弊社においても２、３年前からクラウドに近いシステムのセキュリティ監査の案件が、増えてきており、これらの実施例を通じて、今後ますますの普及が見込まれるクラウドサービスに向けて、情報セキュリティ監査における今後の課題について考察する。

２．情報セキュリティ監査のモデルケース

弊社が実施したセキュリティ監査について、監査対象または内容を分類し、モデルケースとして下記に4種類に分け、その実施内容をモデルとして示す。

２．１ 既存システムからASPサービスへの移行

当モデルケースは、自設置汎用機による既存システムから、ASP サービスへの切替えの際、ASP 事業者のシステム運用について情報セキュリティ面で問題がないかを点検評価するものである。重要情報を外部に委託している場合は、契約書、事業者の説明資料等で納得しているだけでなく、重要情報の情報セキュリティの確保に問題がないかを第三者の視点で点検・評価することが望ましい。監査はデータセンターの運用を中心に行い、公的な標準ガイドライン(6)と監査人の知見に基づいて推進する。

１）セキュリティ監査実施の流れ

①現状システムの把握/分析

システム運用組織体制、システム構成図、障害時連絡網等で現状システムを把握し、利用者サイトの問題認識を突き合わせることで監査のポイントを整理する。

②現地調査項目の作成

公的な監査ガイドライン(6)のうち、「物理的セキュリティ」、「技術的セキュリティ」、「運用セキュリティ」から、情報システムの運用保守に関わる項目を中心に選定する。加えて、利用部門およびデータセンター側の情報セキュリティポリシー、実施手順書と①で把握した観点より調査項目を作成する。

③現地調査

調査項目について、ドキュメント調査、システムの運用管理担当者へのインタビュー、データセンターにおける現地視察および技術診断（アタックテスト）により確認を行う。

④評価・分析・監査報告書作成

調査結果を整理、評価し、問題点を分析し原因と対策を検討する。それらを監査報告書にまとめ、監査報告会（利用者側、提供業者出席）を実施する。

２．２ ASP提供業者とのSLA契約の評価

ASP サービスの利用者と提供業者間のSLA（Service Level Agreement）契約【３】についてのモデルケースである。ASP･SaaS サービス契約においてSLA契約は重要視されている事項である(7)ことから、個別のモデルケースとして取り上げる。

１）サービスレベルの評価について

SLA に基づきSLM（Service Level Management）【４】を構築・運営することにより、サービス利用者側は、期待通りのサービスを享受することが可能となる。また、サービス提供者側にとっては、提供責任を明確にし、適切に対応したことを証明することができる。SLM は、以下のような段階を経て継続的な管理を行うことを通じて、サービスレベルを改善する(8)。

①導入段階

SLM の導入段階においては、重要なサービスの洗い出し、そのサービスについてのレベルの設定、サービスレベルの未達時における対応方法の設定、その他SLAに基づく運営ルールの設定等を行う。

②定着段階

SLM が定着した段階では、サービスレベルの定期的な監視、異常時のサービス提供者による適切な対応、サービスレベル状況と異常時対応などの定期的な報告が行われ、それに基づいてSLA を改善するための検討が行われる。

③改善段階

この段階では、SLM 自体を改善するための議論が、サービス利用者とサービス提供者の間で行われ、SLM 自体の継続的な改善が実施される。

２）SLA の評価と分析

①予備調査と分析

契約書の入手と分析・サービスレベル関連の報告書、その測定方法の分析を実施する。

②SLA の評価項目の妥当性の検証

公的なガイドライン(9)からSLA 契約書の評価項目を洗い出し、契約書の項目評価判定を実施する。

③SLA 契約書の改善案検討

単純見直しと検討を要する項目に分け、それぞれ分析と改善案を作成する。また、SLM の構築と運営の提言を行う。

④報告書の作成と報告会

上記結果を記述した報告書を作成し、報告会を実施する。

３）評価後の改善提言

①SLA 契約の見直し提言

単純な表記見直しと検討を要する事項に分けて提言する。前者は、誤解を与える可能性のある用語見直し等であり、後者は、レスポンスの計測方法および数値化に関する見直し等で、見直し案も含めて提言を行う。

②SLA の定着化への提言

SLA を定着させるための方策、すなわち測定/評価/改善といったマネジメントサイクルを回すことのできる方策を提言する。また、SLM 委員会の設置等、体制改善についても言及する。

２．３ ASP事業者で問題が発生しているケース

システム安定稼動とセキュリティインシデントに関して、ASP 事業者で実際に問題が発生している事例を想定したモデルケースを示す。

１）セキュリティ監査実施の流れ

①問題点の把握

システムインフラ・アプリケーション構成・障害管理表等と過去からのシステム変更の履歴を把握し、問題発生の原因を推測する。

②現地調査項目の作成

①で把握した概要と公的なガイドライン(3)(7)をもとに「サービスの契約内容」、「安定稼動」、「機密保護」、「アクセス権管理」等の観点から調査項目を選定する。そこに、監査人が推測した問題発生原因をふまえた調査項目を追加する。

③現地調査

現地調査項目について運用センター、データセンターにて、ドキュメント精査、運用管理担当者へのインタビュー、現地視察により確認する。また、必要に応じて脆弱性診断も実施する。

④評価・分析・監査報告書作成・報告会

調査結果を整理、評価し、問題点を分析し原因と対策を検討する。それらを監査報告書にまとめ、サービス利用者側とサービス提供業者が出席する監査報告会を実施する。

２．４ インフラを借用したケース

本ケースは、コンピュータ関連費用を削減を狙い、インフラをベンダー持ちとし、設置環境等は、サービス利用者が提供したケースの情報セキュリティ監査である。このケースはある意味でプライベートクラウドに近い形態である。

このケースは、通常の情報セキュリティ監査の手順で行う。ただしベンダーとサービス利用者の契約関係の確認、ベンダーの監査への協力が必須である。

２．５ まとめ

ここまでのモデルケースのとおり、ASP 提供業者への監査は、通常のセキュリティ監査と同様に進めていく事ができるといえる。ただし、基準・ガイドラインは監査対象システムの特性・課題に応じて柔軟に選択する必要がある。また、ASP 事業者とサービス利用者の間で監査実施に関する契約が存在しない場合、監査実施が困難となる事が想定される。弊社の監査事例においても、ASP 事業者側が監査実施に強い拒否反応を示したケースがあった。最終的には、サービスの利用企業（監査依頼者）からの強い働きかけにより監査を

実施することができたが､監査の実施を確実に行うためには監査実施に関する契約が不可欠である。

３．クラウドコンピューティングにおける情報セキュリティ監査の課題

クラウドにおけるセキュリティについては既に多方面から、様々な課題が指摘されている(1)(10)(11)(12)(13)(14)(15)(16)。その中からセキュリティ監査の実施にあたって特に関連が深いと考えられる内容と、弊社の監査事例および調査結果をもとに、課題を挙げる。なお、ここでは利用者を限定しないパブリッククラウドを前提として記述する。

３．１ 事業者の監査協力

クラウド事業者とサービス利用者の間で監査実施に関する契約が存在しない場合、監査実施が困難となる。クラウド事業者側の監査への対応条件に関しては事前に明確しておく必要がある。

３．２ データの保管場所

データの保管場所が海外である場合、そのデータは現地の法律に準拠した扱いを受けることになる。例えば米国の通称「愛国者法」(17)では捜査当局が米国に設置されているサーバ上のデータを調査対象とすることを認めている。また、EU のプライバシー保護に関する法律(18)では、EU からの個人情報の持ち出しが制限されている。

３．３ データのインテグリティ維持

Google、Amazon をはじめとする主要なクラウド事業者においては、「分散キーバリュー・ストア（Key-Value Store）型」のデータベースが広く利用されており(19)(20)、データの一貫性の保証が弱いと考えられる【５】(1)。このことは、データ管理についてシステム管理基準(21)に記載されている「データのインテグリティを維持すること」を満たさない可能性がある。

３．４ 委託先の監督責任

データの管理がクラウド事業者によって行われている場合でもデータの安全性は最終的に利用者が責任を持つ必要がある。例えば、大量の個人情報を含むデータをクラウドで管理する場合、個人情報保護法第22 条の「委託先の監督義務」が適用される。利用者には、クラウド事業者が個人情報の保護水準を満たしていることを評価する義務が生じる。

３．５ 利用者間の環境の分離（仮想化技術の利用）

パブリッククラウドでは、仮想化技術を利用して、複数の利用者によって、ネットワーク、ストレージなどのシステムの基盤環境が共有されている。そのため、一部利用者の仮想環境上で発生した不正アクセスであったとしても､仮にネットワーク機器の設定が不適切等某かの理由で利用者ごとの環境が適切に分離されていない場合､情報漏えいのリスクがある。ハイパーバイザーの脆弱性を悪用した不正アクセスのリスクも否定できない。

また、不正アクセス等が発生した場合、全ての利用者の環境に影響する可能性がある。

監査実施にあたっては、クラウド事業者がクラウドコンピューティング環境構築にあ

たり、仮想化技術を適切に利用し、ネットワークセキュリティをいかに確保しているか、確認する技術が求められる。

また、実態としては複数のユーザがひとつの環境を共有することになる。クラウド事業者は「単一ユーザ」ではなく「複数ユーザ」前提でのキャパシティプランニングに基づく業務継続性確保実施が求められ、監査実施にあたっても留意すべき点となる。

３．６ 効率的な監査の実施

2008年度に「ASP/SaaS安全・信頼性に係る情報開示認定制度」が開始し、事業者の情報セキュリティ対策状況を当該制度のサイトより確認することが可能である。しかし、開示されている情報はあくまでも事業者の自己申告による内容である。

そこで、利用者側に対してクラウド事業者における情報セキュリティ対策の実態を公開し、安全性を示すことが今後求められることも考えられる。

クラウド事業者が利用者からセキュリティ監査を要求された場合、その都度監査を実施するのは現実的ではない。効率的な仕組みを検討する必要がある。例えば、内部統制においては業務委託先が用意した内部統制報告書（SAS70、18 号監査報告書）を元に業務委託先の統制を評価できるという仕組みが利用されている。

情報セキュリティ監査においても、クラウド事業者が外部の情報セキュリティ監査人に作成依頼を行って提出された監査報告書を利用者それぞれに開示することで、利用者からの監査要求に応える仕組みが普及すれば効率的な監査が実施可能になる。

３．７ 必要と考えられるチェック項目

モデルケースで示したように、情報セキュリティ監査の実施にあたっては、標準的な基準･ガイドラインと、委託契約（アウトソーシング）に関連した各種ガイドラインと組み合わせる事で一応の対応が可能である。しかし、これらの基準・ガイドラインはクラウドの特性を十分に加味して作成されたものではない。本格的にクラウド事業者のセキュリティ監査を実施するにあたっては、未整備な点が多いといえる。ここまで挙げた課題をもとに、必要と考えられるチェック項目の例を示す。

１）監査の実施および監査資料の提供に関しての取り決めが契約書に明記されているか
２）データ保管場所が明確になっているか
３）データの一貫性が維持されるか（要求水準を満たすか）
４）利用者間の環境が適切に分離されているか
５）情報セキュリティに関する公的認証を取得しているか

４．まとめ

これまで考察したように、クラウド事業者に対するセキュリティ監査も、通常のセキ　ュリティ監査と同様の手順で進めることになると考えられる。しかし、現状の基準・ガイドラインはクラウドの特性が十分に加味されてはおらず、これに基づいて民間の監査会社が対応可能な範囲は限定的であるといえる。クラウド事業者に対する監査を本格的に実施す

るにあたっては、前述の課題をふまえ、監査実施の仕組みも含むクラウド環境に見合った情報セキュリティ監査の基準・ガイドラインの整備が必要であったが、今年の4月、経済産業省から「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」(16)が発表された。更に不幸なことであるが、東日本大震災が発生し、インターネット上のメールシステム、バックアップデータ保管のクラウドサービスが、注目を集めている。

国内クラウドサービス市場予測によると、「2011年の国内クラウドサービス市場規模は、前年比成長率 45.6%増の660億円」であり、「東日本大震災の影響によってクラウドサービスの需要が拡大、2015年の同市場規模は、2010年比5.6倍の2,557億円」という結果が出ている。

以上のことから今後のより安価で安心、安定なシステムとして、クラウドコンピューティング注目され、種々なサービス形態が提案され、その活用が定着していくにちがいなく、セキュリティ監査においても更に、それに向けての適格で柔軟で、かつ高度な監査が要求されるものと考える。

（本論文は、日本社会情報学会関西支部第１９回研究会（2010年度実施）における「ASP・SaaSに対する情報セキュリティ監査をふまえたクラウドコンピューティングに対する一考」研究発表予稿を改訂したものである。）

注

【1】「メリットのほうが大きい」との回答は17%、「同等」は38%であった。

【2】従業員300 人以上の企業に勤める社員で、社内向のソフトウェア開発、システム開発・運用・保守の担当者500 人を対象にWeb アンケートにより調査を実施。

【3】SLA(Service Level Agreement)：サービスの提供者と利用者との間でのサービス水準に関する合意。サービスの内容・範囲・品質・達成目標などを記述する。

【4】SLM(Service Level Management)：SLAを締結し、その合意内容が適正に実現され、状況の変化に応じて柔軟に運用するように、委託者と提供者間で取り決められた運営の仕組み(ルール、プロセス、体制)を構築・運営すること。

【5】分散キーバリュー・ストア型のデータベースにおいては「eventual consistency(結果としての一貫性)」という考え方が採用されているため、RDB(リレーショナルデータベース)と比較して、データの一貫性の保証が弱い。

参考文献等

(1)情報処理推進機構(2010)
クラウド・コンピューティングの社会基盤に関する研究会報告書(2010.3)
(2)National Institute of Standards and Technology(2009)
The NIST Definition of Cloud ComputingVer.15(2009.10)
(3)総務省(2008)
ASP・SaaS における情報セキュリティ対策ガイドライン(2008.01)

(4)Information Systems Audit and Control Association(2010)
ISACA IT Risk/Reward Barometer(2010.3)
(5)経済産業省(2009)
情報システム・ソフトウェアの信頼性及びセキュリティの取組強化に向けて～豊かで安全・安心な高度情報化社会に向けて～ 中間報告書(2009.5)
(6)総務省(2007)
地方公共団体における情報セキュリティ監査に関するガイドライン(2007.7)
(7)経済産業省(2008)
SaaS 向けSLA ガイドライン(2008.1)
(8)情報処理推進機構(2004)
情報システムに係る政府調達へのＳＬＡ導入ガイドライン(2004.03)
(9)総務省(2003)
公共IT におけるアウトソーシングに関するガイドライン(2003.03)
(10)University of California Berkeley(2009)
Above the Clouds: A Berkeley View of CloudComputing(2009.2)
(11)Cloud Security Alliance(2009)
Security Guidance for Critical Areas of Focus inCloud Computing V1.0 (2009.4)
(12)Cloud Security Alliance(2009)
Security Guidance for Critical Areas of Focus inCloud Computing V2.1 (2009.12)
(13)National Institute of Standards and Technology(2009)
Effectively and Securely Using the CloudComputing Paradigm(2009.10)
(14)Gartner Inc.(2008)
Assessing the Security Risks of CloudComputing(2008.6)
(15)経済産業省(2009)
平成21 年度新世代情報セキュリティ研究開発事業 (クラウドコンピューティングセキュリティ技術研究開発)公募仕様書(2009.7)
(16)経済産業省(2011)
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(2011.4.1)
(17)IDC Japan(2011)
プレスリリース「大震災の影響を考慮した国内クラウドサービス市場予測を発表」(2011.6.28)
(18)総務省 (2009)
データセンターの安全・信頼性に係る情報開示指針 (2009.2.26)
(19)総務省 (2008)
ＡＳＰ・ＳａａＳの安全・信頼性に係る情報開示指針 (2008.11.27)