3ZE-06

SaaS利用企業におけるSaaSに起因するビジネスリスクの影響分析

今井 和人† 大木 榮二郎‡

工学院大学大学院 情報学専攻† 工学院大学 情報学部‡

1. はじめに

1.1. 研究背景

PC やスマートホン，タブレットなどの普及やコストの圧縮や即時性などのメリットにより，企業や個人の利用拡大している．また，クラウドサービスのセキュリティ対策においても，専門的な能力を持った事業者側で管理するため，自力で管理を行うよりも質の高いセキュリティ対策を実現できる可能性がある[1]．しかし，クラウドサービスは管理のもとで他の利用者とコンピュータ資源を共有する．そのため，情報の機密性，完全性，可用性について懸念されている．これに伴い，国内のクラウド環境における情報セキュリティには，国家標準である JIS Q 27002:2006 に基づく管理策の実施が推奨されており，実際に多く利用されている[2]．しかし，クラウドを利用しない理由のセキュリティに不安があるという項目が平成 22 年から平成 25 年までで割合がほとんど変わらず，懸念を払拭できていないことがわかる．

1.2. 研究目的

本研究では，実際のクラウドサービスにおける障害からクラウドサービスのセキュリティ管理策を分析し，セキュリティ対策とビジネスとの関係を明らかにすることを目的とする．

利用者がクラウドサービスの情報セキュリティ対策に関して懸念をしているため，クラウドサービスの情報セキュリティについて利用者が信頼できる環境を整える必要がある．そのため，セキュリティ対策とビジネスリスクの関係を明らかにすることにより，今後のクラウドサービスの利用者と事業者が互いに理解できる枠組みを検討することつながる．

2. 研究手法

本研究では大きくわけて 3 つの手順を用いて過去に発生したクラウドサービスにおける障害の分析を行う．

A SaaS User's Focusing on the Relationship between SaaS Service Structure and User's Busines Process

† Kazuto Imai Major of Informatics, Graduate School of Engineering, Kogakuin University

‡ Eijiroh Ohki, Faculty of Informatics, Kogakuin University

1)JIS Q 20000 の適用

過去に発生した実際のクラウドサービスにおける障害のインシデント原因に JIS Q 20000 を適用した場合の JIS Q 20000 のセキュリティ対策としての有効性を確認する．

2)クラウド抽象化構造の適用

過去に発生した実際のクラウドサービスにおける障害の原因をクラウド抽象化構造に適用し，クラウドの構造内において原因箇所を特定する．

3)ENISA リスクの適用

クラウドコンピューティングにおける ENISA のリスクを用いて障害のインシデントからビジネスリスクを特定する．

3. JIS Q 20000 の適用

3.1. JIS Q 20000 の有効性

トレンドマイクロ社の 2011 年の調査から国内外のクラウドサービス導入における主要な阻害要因は，クラウドインフラ，データの安全性に関する懸念が約 50%，クラウドコンピューティングサービスのパフォーマンスと可用性約 48%という結果がでており，情報セキュリティにおいて利用者の可用性への期待も見受けられる[3].

そのため，顧客が求める IT サービスの安定提供や品質向上をはかることができる JIS Q 20000 の管理策はクラウドサービスの管理策として有効であると推測した．現状の管理策に JIS Q 20000 の管理策を取り入れることで顧客にとってより有効な管理ができることを示す必要がある．したがって，クラウドサービスにとって JIS Q 20000 の有効性を検証する．

現状のクラウドサービスのセキュリティ管理策として推奨されている管理策で対策可能であるか確認することや JIS Q 20000 の管理策との比較を行うために，同時に JIS Q 27002 の管理策とクラウドコンピューティングのために策定されたクラウド情報セキュリティ管理策についても適用を行う．

3.2. 障害の適用管理策数

各管理策への適応は章，節ごとに行った．適用した結果，各管理策の障害適用管理策数(Number of Controls)を図 1 に示す．

障害に適用された JIS Q 20000 の管理策数は

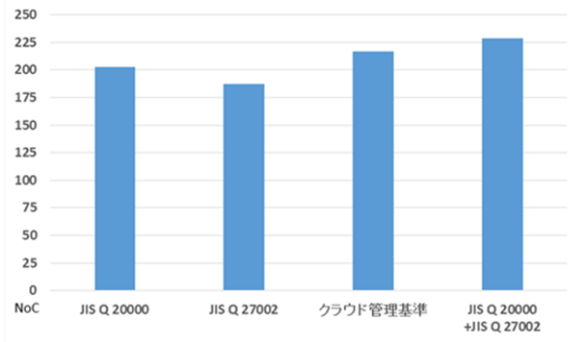

図 1 障害の適用管理策数

JIS Q 27002 の管理策数より多いことがわかり，適用されたクラウド管理基準の管理数は JIS Q 27002 の管理数に比べ増えていることもわかった．また，管理策に重複のない JIS Q 20000 と JIS Q 27002 の合計がクラウド管理基準よりも多いことがわかった．

4. クラウド抽象化構造の適用

クラウドの構造においてインシデントの発生箇所を把握するためにインシデントの原因からクラウドの抽象化構造に適用する．適用するための抽象化構造は JASA のモデルを用いる．

障害の抽象化構造の適用数(Number of Incident)を図 2 に示す．運用ルールや設計ミスなどが多く，その他の項目が目立つ．クラウドの構造外の問題が多いと結果となった．

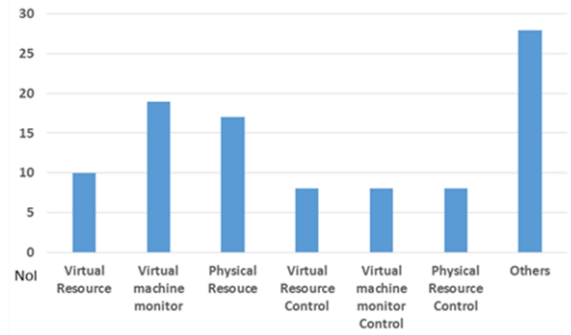

図 2 抽象化構造適用数

5. ENISA リスクの適用

管理策とビジネスリスクの関係を把握するため，3.の適用にて特に適用数の多かった管理策において ENISA のリスクを適用させた．また，抽出したリスクから障害において影響を受けたと推測される資産(Number of Asset)を抽出し，数の多い方から 5 つを図 1 に示す．

また，インシデントにおけるリスクの中には JASA の評価で低と判断されたものも存在し，そのインシデントによって重大な被害も出ている．したがって，リスクの程度が低いものでも度外視できない．

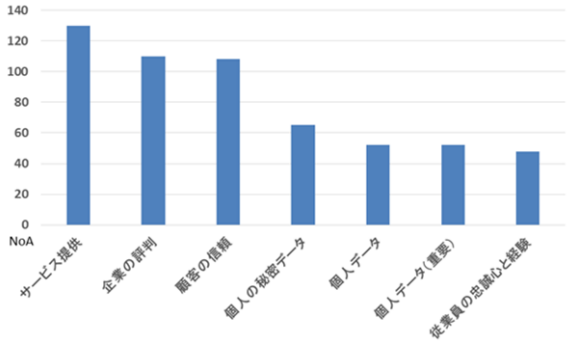

図 3 影響を受けたと推測される資産

6. まとめ

クラウド特有の構造によってインシデントが発生しているということはなく，運用方法，設計，設定ミスによるインシデントが障害に繋がっていることがわかった．そのため，現在クラウドのセキュリティ管理策のベースとなっている JIS Q 27002 は管理策として効果的であることがわかった．したがって，JIS などの管理策で運用方法を確立することで障害が起こる確率を大幅に減らせる可能性がある．また，障害の管理策適用数やサービス提供に影響がでていることから JIS Q 20000 の管理策がクラウドサービスのセキュリティ対策として有効であり，JIS Q 27002 と組み合わせることによって多くのビジネスリスクを回避や低減できることが期待できる．

7. 主要参考資料

[1] IPA，「クラウドコンピューティングのセキュリティその意味と社会的重要性の考察」，http://www.ipa.go.jp/files/000024751.pdf (2015/1 アクセス)

[2] 経済産業省，「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 2013 年度版」，http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf (2015/1 アクセス)

[3] トレンドマイクロ株式会社，「クラウドへの不安：43%の企業がクラウドサービスでセキュリティ問題を経験」，http://www.trendmicro.co.jp/jp/about-us/topics/articles/20130827015010.html (2015/1 アクセス)