Vol.2010-CSEC-51 No.6
2010/12/10

クラウドに関する情報セキュリティの課題の整理～アンケート調査結果からの分析～

服部真[†]　　原田要之助[†]

本稿は，クラウドコンピューティングの情報セキュリティに関する課題をアンケート調査結果から考察したものである．さらに，本調査では，欧州と日本におけるクラウドに関する情報セキュリティの意識動向を比較するために，調査項目をENISA の調査と合わせている．結果としては，日本の組織は，欧州よりもサービス継続性を重視する傾向にあり，クラウドにおける障害発生時の対応に関して懸念を抱いていることなどを明らかにしている．

A study on information security on Cloud Computing - based on survey results -

Makoto Hattori[†] and Yonosuke Harada[†]

This analysis based on survey results on information security for Cloud Computing in Japan. The survey compare with that of EU by similar study by ENISA, and concludes security appetite for cloud computing is not equal in Europe and in Japan. From survey results, we investigate potential important security issues and propose study topics for futures Cloud Computing.

1. はじめに

クラウドコンピューティング（以下,「クラウド」と呼ぶ）は，NIST（米国の National Institute of Standards and Technology）によれば，コンピューティング資源（ネットワーク・サーバー・ストレージ・アプリケーション・サービス）の共有プールへの，オンデマンドなアクセスを可能にする IT の利用形態を指す．NIST はクラウドを Public, Private, Community, Hybrid の 4 つの提供形態と，SaaS, PaaS, IaaS の 3 つのサービスモデルに分類し,「オンデマンドセルフサービス」「ブロードバンドネットワーク」「リソースの共有」「柔軟性」「サービス性能が測定可能」の 5 つの特徴を備えた IT の利用形態と定義している[1].

代表的なクラウドサービスには，Amazon Web Services 社の Amazon S3 や Amazon EC2, Salesforce.com 社の Salesforce CRM や Force.com がある．この他にも Amazon Web Services 社の提供するサービスを自社サービスのインフラとして利用する Right Scale 等のように，ある事業者の IaaS 上で別の事業者が IaaS を提供するサービスも登場している．

また，調査会社の IDC が 2010 年 5 月に発表した報告書「Worldwide Enterprise Server Cloud Computing 2010-2014 Forecast」によると，景気回復とハードウェア老朽化が相まって企業の約半数がクラウドをベースとしたインフラへの移行を検討していると述べている[2]．さらに，ITPro が実施したアンケート調査「2010 年に注目したいマネジメント/情報システム分野の IT キーワード」によると，クラウド関連のキーワードが上位を占めている[3]．このように，クラウドに対する企業の注目は大きくなってきている．

注目が高まる一方で，クラウドの利用を懸念する意見も多い．IDC Japan が 2010 年 6 月に発表したアンケート調査結果「国内クラウドサービス市場ユーザー動向調査結果」によると,「セキュリティへの不安」がパブリッククラウドサービスの阻害要因として最も大きいと述べている[4].

本稿では，クラウドのセキュリティに対する課題を明らかにするために，日本国内の 4500 組織を対象に実施したアンケートついて調査を行った．調査結果をまとめ，クラウドに関する課題をまとめた．

2. クラウドセキュリティの課題

クラウドのセキュリティ上の課題については様々な組織で研究が進められている．米国のクラウド関連事業者を中心に結成された CSA（Cloud Security Alliance）は，クラウドにおけるセキュリティのベスト・プラクティスの普及促進を目指し，ガイドラ

[†] 情報セキュリティ大学院大学
Institute of Information Security

イン「Security Guidance for Critical Areas of Focus in Cloud Computing」を発表している．欧州においては，情報通信分野のセキュリティの研究機関である ENISA（European Network and Information Security Agency）で，表 1 に示す通り，クラウドのリスクを評価して報告書にまとめている[5] ．我が国においては，経済産業省のクラウド・コンピューティングと日本の競争力に関する研究会[6]や総務省のスマート・クラウド研究会[7]などが報告書を発表している．

様々な組織がクラウドについての研究を実施しているが，ENISA のように，クラウドのリスクの評価（High, Medium, Low による分類）をしているケースは稀である．しかしながら，この評価は ENISA が，欧州の企業に対して行った調査をもとに主観的に分析したものであり，前章で述べた IDC のアンケート結果が示す，実組織における「セキュリティへの不安」の実態は明らかになっていない．

表 1　ENISA の挙げるクラウドのリスクの一部

分類	リスク（評価）
組織的リスク	ロックイン（High），ガバナンスの喪失（High），コンプライアンス対応（High），サービスを共用するためコーポレートレピュテーションを低下させる（Medium），クラウドサービスのサービス停止及び障害によるサービス中断（Medium），クラウド・プロバイダの買収（Medium），サプライ・チェーンのトラブル（Low）
技術的リスク	リソース過不足の問題（Medium），サービスを共用するため他のユーザー企業の影響を受けるリスク（High），内部者の悪意，管理者の特権濫用のリスク（High），管理者機能の悪用によるリスク（Medium），データ通信経路途中におけるリスク（Medium），データ漏洩（Medium），事業者のデータ消去漏れのリスク（Medium），DDoS のリスク（Medium），EDoS のリスク（Medium）
法的リスク	法令による命令や証拠保全（High），裁判管轄の違い（High），データ保護に係るリスク（High）ソフトウェアライセンスに係るリスク （Medium）
共通事項	ネットワークのダウン（Medium），ネットワーク管理ミス（High），ネットワークトラフィックの経路変更（Medium），権限奪取（Medium），ソーシャルエンジニアリング攻撃（Medium），運用ログの滅失又は漏洩（Low），機器の盗難（Low），自然災害（Low）

3. クラウドセキュリティのアンケート調査

3.1 アプローチ

クラウドのセキュリティに関する我が国の実組織の意識動向を明らかにすることを目的に，アンケート方式による調査を実施した．

アンケートの調査項目の検討にあたっては，ENISA の報告書[5]および，経済産業省の「SaaS 向け SLA ガイドライン」[8]等を参考にした．これらの文書を参考にした理由は次の通りである．

- ENISA と同様の項目を日本の企業が評価する場合には，「例えば地震の多い日本の場合は自然災害に対する評価が高くなる（より問題視する）など，結果が異なるであろう」という仮説のもとで，欧州におけるセキュリティの意識動向と日本におけるセキュリティの意識動向の比較ができる
- リスク項目および，SLA 項目は，多様かつ具体的であり，クラウドに対する日本の組織の意識動向，懸念や期待を具体的な言葉として表現する際の参考になる
- 公開されている文書を参考にすることで，被検組織の調査項目に対する理解を期待できる
- 公開されている文書を参考にすることで，調査結果を公表した際に，結果を参考にしたい組織の理解を得やすくなる

3.2 調査概要

アンケート調査は 2010 年 8 月 1 日～31 日に実施した．実施方法は郵送で，調査対象は日本国内の上場・非上場企業，行政機関，大学を中心とする前 9,000 組織からランダムに選んだ 4,500 組織である．有効回答数は，設問によって異なるが，凡そ 305～316（約 7%）であった．アンケート調査項目は，[9]を参照のこと．

主な調査項目を以下に示す．

(1) 組織の概要（スクリーニング用）：業種，年間売上高，従業員数，保有 PC 台数，情報セキュリティポリシーの有無，情報セキュリティ監査の実施有無，情報セキュリティ事件/事故の発生有無/頻度，IT 関連予算額の割合，情報セキュリティ教育の実施状況等

(2) クラウドの利用動向：クラウドの利用有無，利用（を予定）している事業者，利用（を予定）しているサービス等

(3) クラウド事業者へのリスク評価：自組織管理下にあるシステムとクラウドとの脅威の差異，従来のアウトソーシングに対する脅威とクラウドとの脅威の差異，ENISA の挙げるリスク評価項目と重視するもの

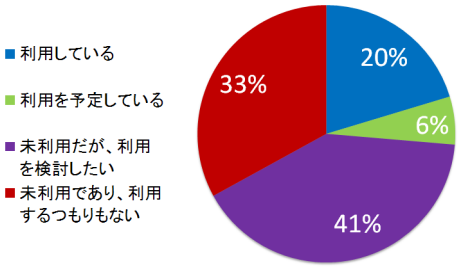
(4) クラウド事業者の選定要因：クラウド事業者を選択する上で重視する項目，現在利用中のサービスの満足度，クラウドに求められる SLA 項目等

3.3 調査結果

(1) クラウドの利用動向

クラウドの利用有無と予定に関する設問の回答結果を図 1-1 に示す．

「利用している」「利用を予定している」「未利用だが，利用を検討したい」を選択した利用意向のある組織の数が，全体の 2/3 を占めることが分かる．

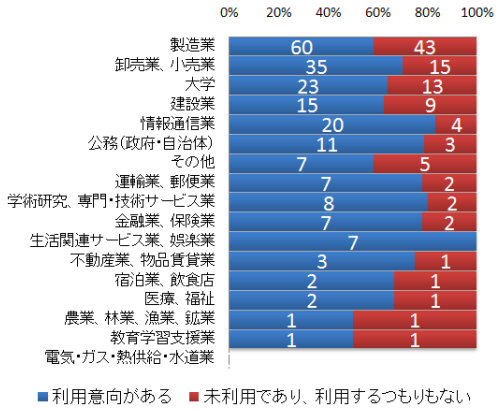


単位：%
N=315，単数選択

図 1-1 クラウドの利用有無

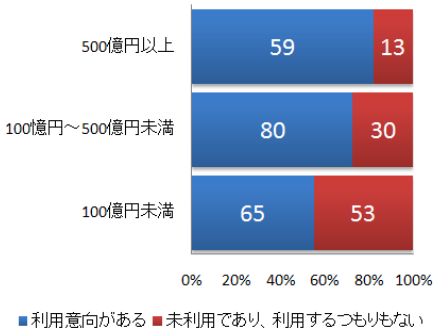
図 1-2 と図 1-3 は，クラウドの利用意向がある組織の数と，「未利用であり，利用するつもりもない」を選択した組織の数の割合を示す．なお，図 1-2 は業種別，図 1-3 は年間売上高別の割合を示す．

組織の業種や年間売上高によって，クラウドの利用意向に多少の違いがあることが分かる．特に，年間売上高が 500 億円以上の大企業の利用意向が強いことが分かる．



単位：組織
N=312，単数選択

図 1-2 業種別のクラウド利用意向の割合

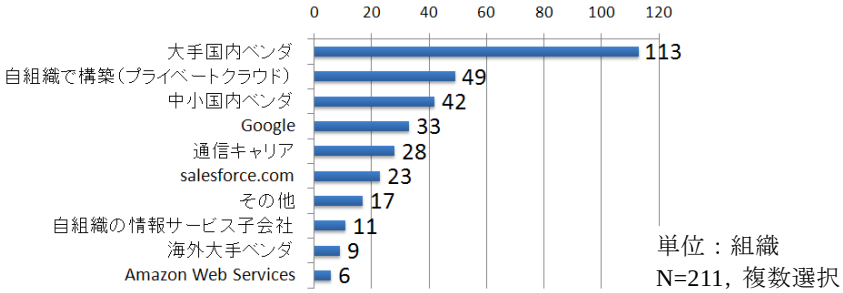


単位：組織
N=300，単数選択

図 1-3 年間売上高別のクラウド利用意向の割合

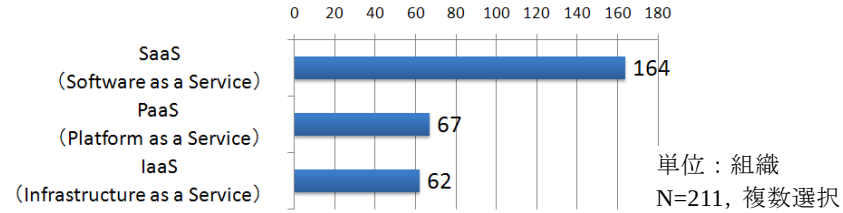
図 1-4 と図 1-5 は，利用（を予定）しているクラウド事業者とサービスに関する設問の回答結果である．

大手国内ベンダのクラウドへの選好が強いこと，および SaaS の利用（を予定）している組織が多いことが分かる．



単位：組織
N=211，複数選択

図 1-4 利用（を予定）しているクラウド事業者



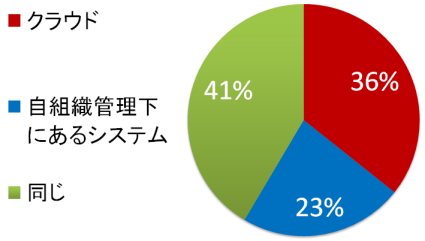
単位：組織
N=211，複数選択

図 1-5 利用（を予定）しているクラウドサービス

Vol.2010-CSEC-51 No.6
2010/12/10

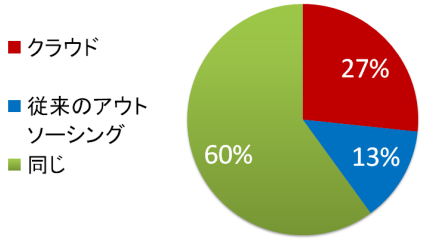
(2)　クラウド事業者へのリスク評価

図 2-1 はクラウドと自組織管理下にあるシステムで，セキュリティ上の脅威はどちらが大きいと感じるかについての回答結果である．図 2-2 は，クラウドと従来のアウトソーシング（ホスティング）で，セキュリティ上の脅威はどちらが大きいと感じるか聞いた設問の回答結果である．どちらもクラウドの脅威の方が大きいと感じる傾向にあることが分かる．一方で，「同じ」という回答も多く，特にクラウドと従来のアウトソーシングを比較すると，その傾向が強いことが分かる．



単位：%
N=311，単数選択

図 2-1　感じる脅威の大きさの比較＜クラウドと自組織管理下システム＞



単位：%
N=311，単数選択

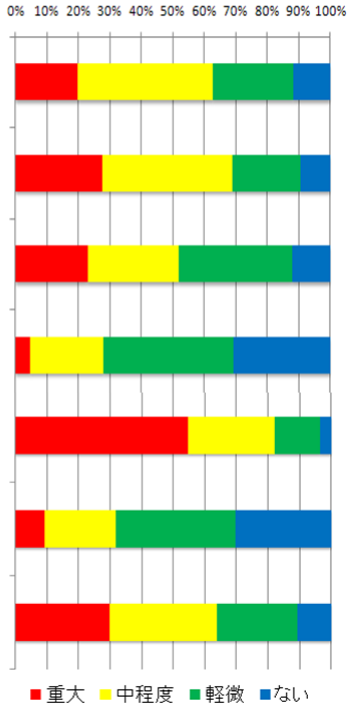
図 2-2　感じる脅威の大きさの比較＜クラウドと従来のアウトソーシング＞

図 2-3 は，クラウドの組織的リスクに対する ENISA の評価[5]と，同リスクを対象組織ではどのように評価するか聞いた設問の結果を比較している．ここでは，ENISA が High と評価する「LOCK-IN」や「LOSS OF GOVERNANCE」は，ENISA の評価結果に比べ，重大と見なされていない（重大が 25%で，中程度が 40%であることから重大とは言えない）ことが分かる．一方，ENISA の評価結果で Medium となっている「CLOUD SERVICE TERMINATION OR FAILURE」（重大が 53%，中程度が 27%で，重大と言える）や「SUPPLY CHAIN FAILURE」（重大が 30%，中程度が 35%）を重視することが分かる．以上の結果からは，日本の組織は，欧州よりもサービス継続性を重視する傾向にあることが伺える．

ENISAのリスク評価

リスク	評価
LOCK-IN 事業者に囲い込まれて、後日、事業者を変更できなくなってしまうリスク	High
LOSS OF GOVERNANCE 事業者にすべてを任せてしまい、自組織で対応できなくなるリスク	High
COMPLIANCE CHALLENGES 事業者のコンプライアンス違反で、自組織も違反になってしまうリスク	High
LOSS OF BUSINESS REPUTATION DUE TO CO-TENANT ACTIVITIES 同じ事業者を利用する競争相手との差別化ができなくなるリスク	Medium
CLOUD SERVICE TERMINATION OR FAILURE 事業者がサービスを中断したときに、自組織のビジネスへのリスク	Medium
CLOUD PROVIDER ACQUISITION 事業者が買収されて、競合相手の傘下に入ってしまうリスク	Medium
SUPPLY CHAIN FAILURE 事業者が利用している他のクラウド事業者のトラブルの影響を受けて、サービス提供が中断したり、サービス内容が変更されるリスク	Low

アンケート結果



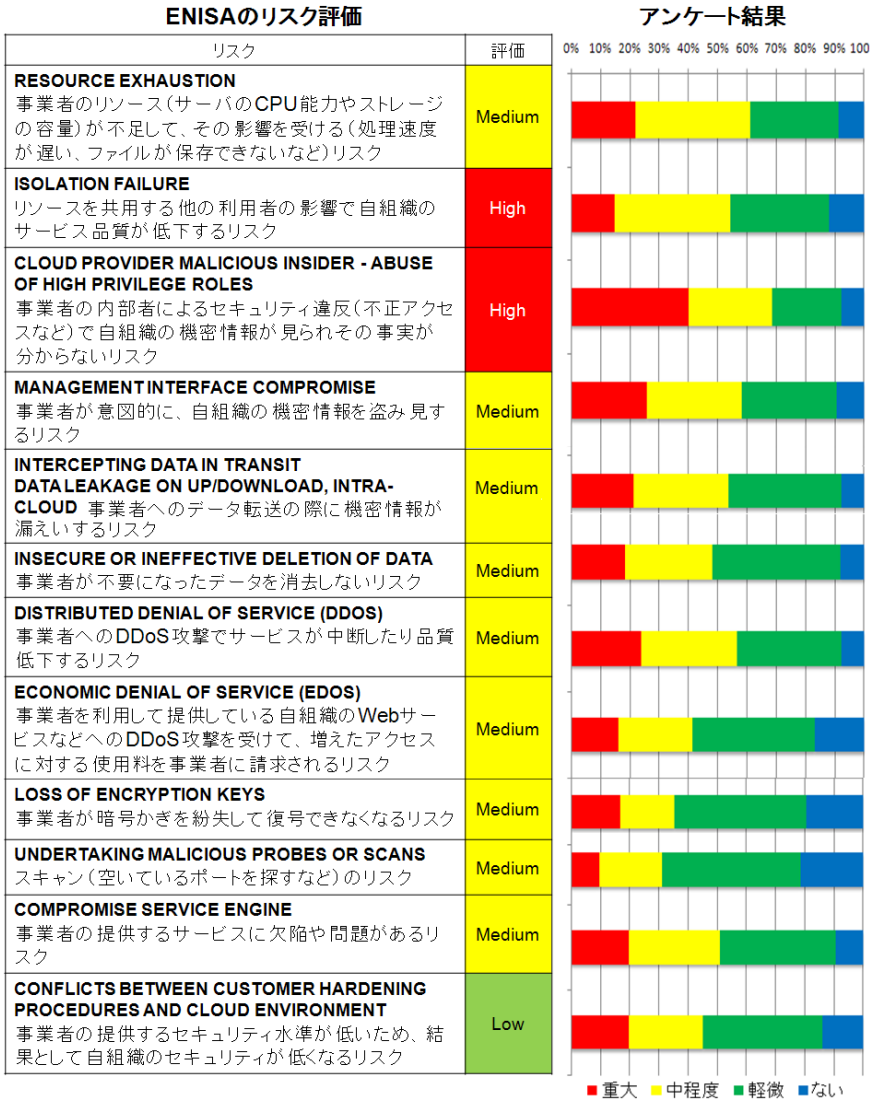
単位：%，N=311，単数選択

図 2-3　ENISA のリスク評価結果と日本の調査結果の比較＜組織的リスク＞

図 2-4 は，クラウドの技術的リスクに対する ENISA の評価結果[5]と，同リスクについて我が国の組織に対する調査結果を比較している．

ENISA が High と評価する「ISOLATION FAILURE」が ENISA の評価結果に比べるとあまり重視していないことが分かる．また，全体的に中程度の評価が多い中で，「CLOUD PROVIDER MALICIOUS INSIDER」は，重要視されている．この項目は，従来から自組織管理外で情報を保管する場合には必須となる課題であり，クラウドにおいても，従来同様に，重要視されていることが分かる．一方，「ISOLATION FAILURE」は，従来からマルチテナントの環境を利用している組織でない限り，クラウド利用時における具体的な悪影響のイメージを想定できていないことが分かる．

Vol.2010-CSEC-51 No.6
2010/12/10

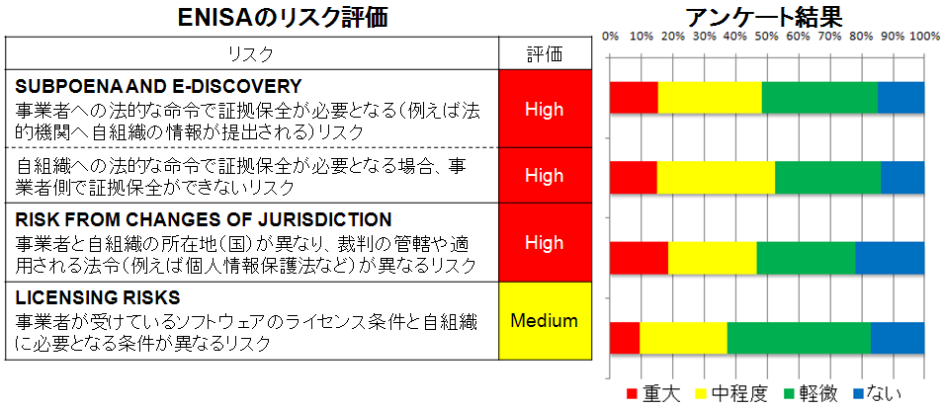


単位：%，N=311，単数選択

図 2-4　ENISA のリスク評価とアンケート結果の比較＜技術的リスク＞

図 2-5 は，クラウドの法的リスクに対する ENISA の評価結果[5]と，同リスクについて対象組織の調査結果とを比較している．図 2-5 からは，多くの組織では，海外に自社のデータが管理されるような観点での法的リスクについての認識が未だ十分ではないことが分かる．

前章の図 1-4 が示す通り，今回の対象組織の多くは国内クラウド事業者の利用を想定しているためか，米国における「E-DISCOVERY」や裁判管轄権の問題である「CHANGES OF JURISDICTION」のリスク[脚注i]を認知する環境にないことが分かる．



単位：%，N=311，単数選択

図 2-5　ENISA のリスク評価とアンケート結果の比較＜法的リスク＞

図 2-6 は，クラウドの共通的リスクに対する ENISA の評価結果[5]と，同リスクを対象組織での調査結果を比較している．

ENISA が High と評価する「NETWORK MANAGEMENT」は，ENISA の評価より軽視されていることが分かる．また，「NATURAL DISASTERS」は欧州と日本における地震・津波等の災害に対する認識の違いから顕著な差が現れることを想定したが，ENISA よりも多少重視する程度であることが分かった．一方で，ENISA が Medium と評価する「NETWORK BREAKS」は，ENISA の評価結果[5]よりも重視されている．

これらの結果からは，日本におけるクラウドのサービスを支えるデータセンターのインフラ，および運用の品質に対する信頼度・期待度は高い．すなわち，組織のサー

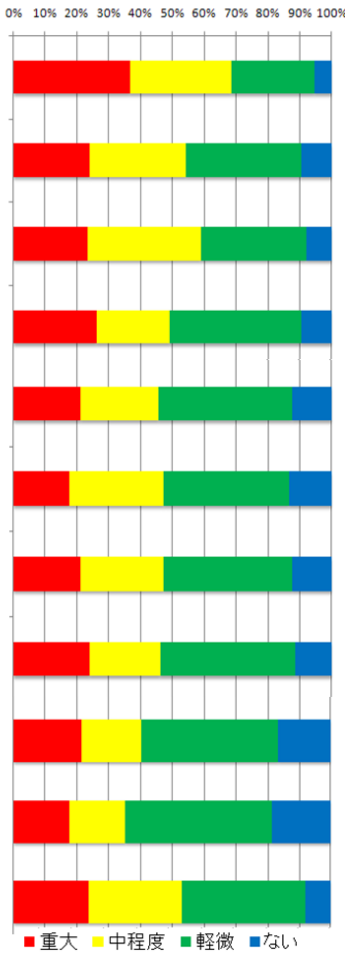
脚注i. ENISA は，データセンターが設置される国によっては，法執行機関や民事訴訟による証拠提出命令により，物理的なハードウェアまたはデータが強制的に没収・開示されるリスクがあることを指摘している[5].

ビスに対する直接的な影響をイメージし易いリスクについては重要視する傾向にあることが分かる．

ENISAのリスク評価

リスク	評価
NETWORK BREAKS 事業者と自組織を結ぶネットワークがダウンするリスク	Medium
NETWORK MANAGEMENT 事業者の運用管理体制が悪く、容量不足や、接続ミスなどが起きるリスク	High
MODIFYING NETWORK TRAFFIC ネットワーク障害の場合、事業者と自組織間の経路変更できないリスク	Medium
PRIVILEGE ESCALATION 事業者のルート権限を奪取されて、自組織情報が盗まれたり、改ざんされるリスク	Medium
SOCIAL ENGINEERING ATTACKS 事業者がソーシャルエンジニアリング攻撃を受けて、自組織に関する情報を開示するリスク	Medium
LOSS OR COMPROMISE OF OPERATIONAL LOGS 自組織サービスが取得しているログを紛失したり、漏えいさせるリスク	Low
LOSS OR COMPROMISE OF SECURITY LOGS 事業者が認証などのセキュリティログを紛失したり、漏えいさせるリスク	Low
BACKUPS LOST, STOLEN 事業者がバックアップファイルを毀損させたり、漏えいさせるリスク	Medium
UNAUTHORIZED ACCESS TO PREMISES 事業者の施設に簡単に侵入でき、機器にもアクセスできるリスク	Low
THEFT OF COMPUTER EQUIPMENT 事業者の機器(サーバ、ストレージなど)が盗まれるリスク	Low
NATURAL DISASTERS 事業者が自然災害を受けてサービスが停止するリスク	Low

アンケート結果



単位：%，N=311，単数選択

図 2-6　ENISA のリスク評価とアンケート結果の比較＜共通的リスク＞

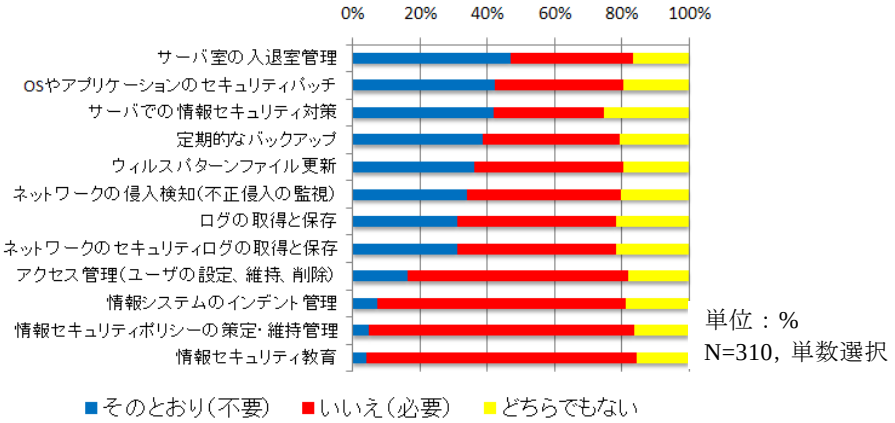
図 2-7 は，クラウドの導入により不要となるセキュリティ対策の調査結果である．

「サーバ室の入退室管理」，「OS やアプリケーションのセキュリティパッチ」，「サーバでの情報セキュリティ対策」が不要と考える組織が多いことが分かる．一方で，「情報システムのインシデント管理」，「情報セキュリティポリシーの策定・維持管理」，「情報セキュリティ教育」についてはクラウドを導入しても不要にならないと考える組織が多いことが分かる．

これらの調査結果からは，サーバ室などの物理セキュリティやセキュリティパッチなどの対策は不要になると考えられている一方で，インシデント管理や教育などのマネジメントや人的セキュリティに関する対策は必要と考えられていることが分かる．

なお，サーバや OS・アプリケーションに関するセキュリティ対策は，利用するクラウドサービスのモデル（SaaS/PaaS/IaaS）によって異なるため，不要か必要かは組織の置かれた状況によって異なるので，結果はあくまでも一般論と考えるべきであろう．

また，ネットワークに関するセキュリティ対策は，クラウドサービスが提供されるシステム内についてはクラウド事業者側で実施されるが，利用者とクラウドサービス間のセキュリティについては依然として利用者側での対策が必要になる．



単位：%
N=310，単数選択

図 2-7　クラウドの導入より不要となるセキュリティ対策

(3)　クラウド事業者の選定要因

図 3-1 は，組織がクラウド事業者を選択する場合に，重視する項目に関する調査結果である．「非常に重視する」が最も多く選択された項目は，「障害が起きた時の対応が早い」であり，次いで「月額（ランニング）費用が安い」と「導入（イニシャル）費用が安い」が選択されている．さらに，「技術力が高い」「アウトソーシングの経験が豊富である」「会社の実績が豊富である」も多く選択されている．

一方で，「広告，宣伝を良く見る」「セミナーなど頻繁に開催している」を重視する組織は少ないことが分かる．

これらの結果からは，クラウド事業者の広報・宣伝活動は重視されず，実績に基づく確実なサービス提供と，費用の安さを重視することが分かる．クラウド事業者は，費用に対する期待に応えるとともに，高いサービス品質を実現することが求められている．

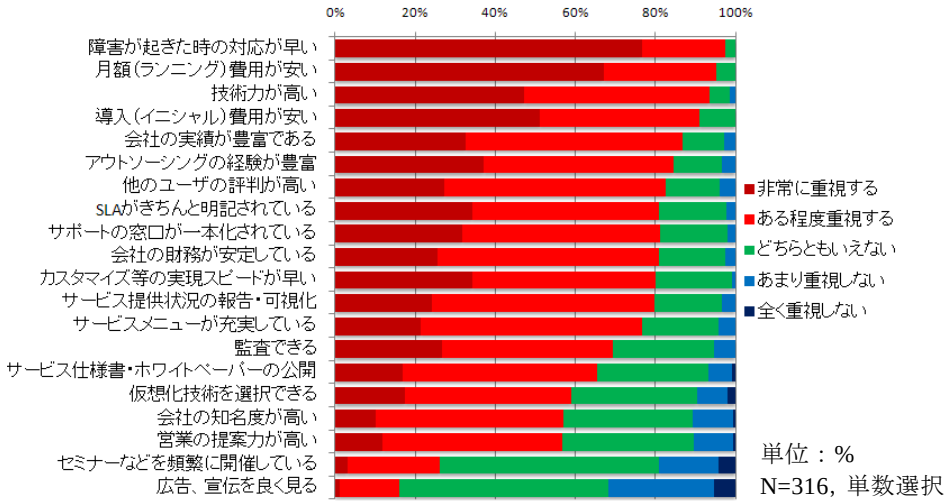


図 3-1　クラウド事業者の選択で重視する項目

図 3-2 は，現在利用中のクラウドサービスの満足度の結果である．「会社の知名度が高い」は，図 3-1 を見ると重要度は低いものの，図 3-2 からは満足度は高いことが分かる．「導入（イニシャル）費用が安い」「月額（ランニング）費用が安い」に対する満足度は高い一方で，不満も伺える．また，「営業の提案力が高い」や「カスタマイズ等の実現スピードが速い」の不満度も高い．

これらの結果からも，費用に対する期待が高いことが分かる．また，「会社の知名度が高い」や「会社の財務が安定している」の満足度が高いことから，クラウド事業者の安定性に対する期待も高いことが分かる．

また，「営業の提案力が高い」に対する不満が多い点は，ウェブ上でサービスの申込みから契約，システムの構築ができるパブリッククラウド（IaaS）においても，なおクラウド事業者に営業力が求められることを示唆している．「カスタマイズ等の実現スピードが速い」に対して不満があることも，従来のシステム開発において求められた顧客対応の柔軟性が求められることを示唆している．

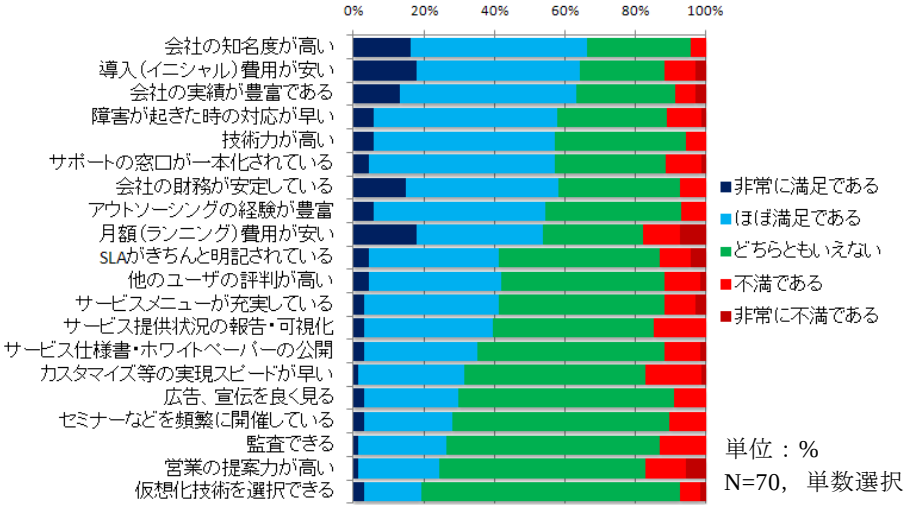


図 3-2　現在利用中のクラウドサービスの満足度

図 3-3 は，クラウド事業者との SLA で特に重視する項目を聞いた設問の結果である．（本項目は経済産業省の SaaS 向け SLA ガイドラインを参考に構成している[8]）．最も多く選択されている項目は「重大障害時の代替手段」である．次いで，「サービス時間」「平均復旧時間」「サービス稼働率」が選択されている．また，「バックアップの方法」や「バックアップデータの保存期間」，「オンライン応答時間」を選択した組織も多いことが分かる．

これらの結果からは，図 3-1 が示す結果と同様に，障害発生時の対応に関する期待の高さが伺える．また，バックアップに関する項目も重視されていることから，障害が発生した場合にも，クラウドに預けたデータへアクセスできることが求められている．すなわち，日本の組織は，信頼性に対する要求が高いことが分かる．

現在，多くのクラウド事業者ではサービス稼働率だけを SLA として取り決めていることが多いが[10]，クラウド事業者は障害発生時の代替手段を用意するとともに，その手段および障害発生時のプロセスを明示し，実施項目を SLA に含めることが期待されている．

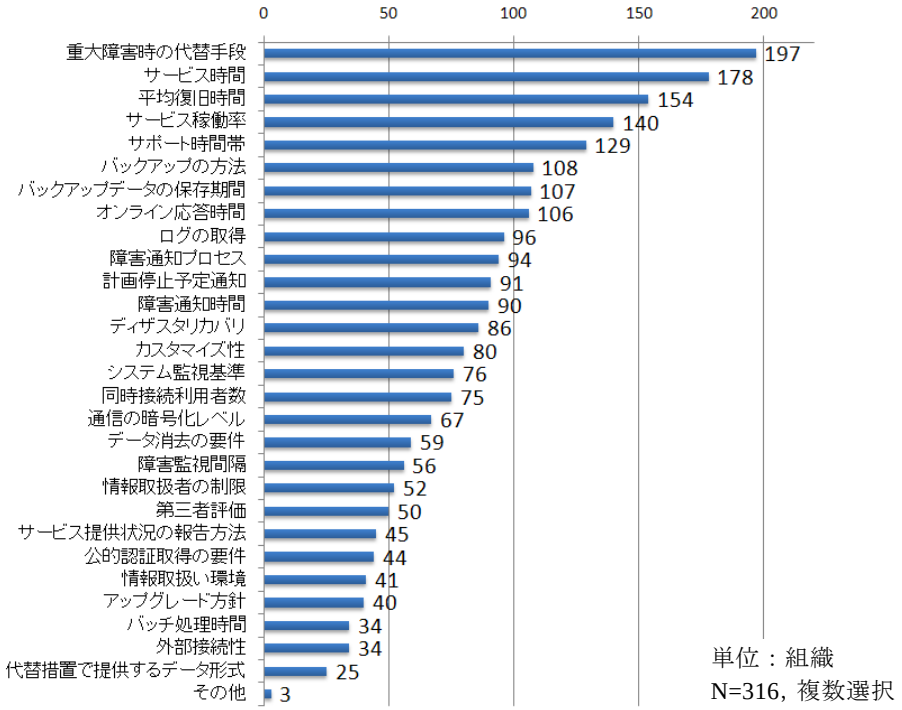


図 3-3　クラウド事業者との SLA で特に重視する項目

4. まとめ

アンケート調査の結果から，日本組織のクラウドの情報セキュリティに関する意識動向は以下のとおりである．

- 年間売上高が 500 億円以上の大企業にクラウドの利用意向が強く，大手国内ベンダおよび SaaS を利用（を予定）している組織が多い
- 多くの組織はクラウドにおける脅威の大きさについては，従来のアウトソーシングとほぼ「同じ」と考えている
- 多くの組織は国内クラウド事業者の利用を想定している
- 多くの組織は国外の法律や裁判管轄権の問題の認識が低い
- クラウドにおける障害発生時の対応に関する懸念と期待が大きく，欧州よりもサービス継続性を重んじている
- 多くの組織はクラウドについてインシデント管理や教育などのマネジメントや人的セキュリティ対策は必要と考えている
- 多くの組織はクラウドにおける障害発生時の対応を SLA に含めることをクラウド事業者に期待している

以上から，クラウドに関する課題は以下のようにまとめられる．

クラウドの課題

（1）クラウドを利用する組織

- 組織は増加する IT コストを低減させる技術として期待しているが，クラウド事業者のセキュリティ対策については不明な点が多く，不安が顕在化している．
- 組織にとって，クラウドは情報セキュリティ対策を無くすものではなく，とくに，インシデント管理や教育などのマネジメントや人的セキュリティ対策は重要である．
- 組織はクラウドを利用するときの SLA について，求めるものを十分に理解していない．今後，クラウド事業者と組織の双者が納得する SLA が必要である．

（2）クラウド事業者

- 事業者は，自社の情報セキュリティやリスクについて，利用組織からの信用を得るためには情報公開が必要である．
- 事業者には，従来の IT サービスと同様の高品質が求められている．とくに，障害時の代替手段やサービス時間，復旧時間などが重要となっている．

（3）共通事項

- クラウドは，グローバルな特徴を生かしたサービスである．この特徴をどのように生かすかについて，利用，提供両面からの検討が必要である．

5. おわりに

本稿では，クラウドに関する情報セキュリティの課題の整理としてアンケート調査結果をまとめ，結果から今後のクラウド事業者，利用組織の課題を考察した．

特に，クラウド事業者においては，今回の調査で明らかとなった「障害時発生時の対応の重要性」など，日本の固有のニーズが顕在化していることを認識する必要がある．具体的な，障害発生時のクラウド事業者および利用組織がとるべき対応については，今後の研究課題である．

謝辞 本研究を実施するにあたりアドバイスや支援を頂いた情報セキュリティ大学院大学の関係各位, アンケート調査にご回答頂いた関係組織の関係者各位, そして, アンケート調査や発表に関して多大なご支援を賜りました日本 IT ガバナンス協会の関係者の皆様に, 謹んで感謝の意を表します.

参考文献

1) Mell, P. and Grance, T : The NIST Definition of Cloud v15 ,National Institute of Standards and Technology (2009) http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
2) IDC, IDC Worldwide Enterprise Server Cloud Computing 2010-2014 Forecast (May, 2010)
3) 田中淳,ITPro ［マネジメント/情報システム］クラウド関連が圧倒的な強さ,「IFRS」も急上昇(2010) http://itpro.nikkeibp.co.jp/article/COLUMN/20100106/342924/
4) IDC Japan, 国内クラウドサービス市場ユーザー動向調査結果を発表 (June, 2010) http://www.idcjapan.co.jp/Press/Current/20100603Apr.html
5) Daniele Catteddu and Giles Hogben, Cloud Computing : Benefits, Risks and Recommendations for Information Security, ENISA (Nov. 2009)
又は, 原田, クラウドコンピューティングのリスクとガバナンスに関する調査・研究について, 情報処理学会誌[小特集] クラウド・セキュリティ, Vol.51, No.12, pp.1-11 (Dec, 2010)
6) 経済産業省, 「クラウドコンピューティングと日本の競争力に関する研究会」報告書(Aug, 2010) http://www.meti.go.jp/press/20100816001/20100816001-3.pdf
7) 総務省, スマート・クラウド研究会報告書(May, 2010) http://www.soumu.go.jp/main_content/000066036.pdf
8) 経済産業省, SaaS 向け SLA ガイドライン(Jan. 2010) http://www.meti.go.jp/press/20080121004/03_guide_line_set.pdf
9) 情報セキュリティ大学院大学, 情報セキュリティ調査の実施について (Aug, 2010) http://lab.iisec.ac.jp/~harada_lab/survey.html
10) 総務省, スマート・クラウド研究会報告書参考資料 別紙 5 (May, 2010) http://www.soumu.go.jp/main_content/000066039.pdf