JEITA

IS－10－技標－ 1

セキュリティ市場・技術調査報告書

2010年3月

社団法人 電子情報技術産業協会

はじめに

本調査報告書は、セキュリティ市場・技術調査専門委員会が、「クラウド/SaaS 時代のセキュリティ技術と関連ビジネス」に関する調査を行い、日本や米国のクラウド/SaaS 市場の動向や情報セキュリティ対策ニーズの状況などからクラウド/SaaS 時代における日本の情報セキュリティ産業の方向性を検討、分析した結果を報告するものである。

近年、ストレージコストの低減や分散処理技術の高度化、通信環境の充実など、安価な ICT 基盤が急速に整備されつつあり、「クラウドコンピューティング」のサービスに注目が集まっている。クラウドコンピューティングは、サーバ等が提供するサービスを、リソースを意識せずにインターネットなどのネットワークを通じて使用できるモデルであり、ユーザは、サーバ設備などの初期投資をせずに、いつでも必要な時に必要なだけ、コンピュータリソースを利用できる。ユーザにとって様々な利点があり、普及が見込まれているが、一方で自社のデータがインターネット上のどこに保管されているかわからないという不安もあり、安全性や信頼性、適法性などのセキュリティ上の課題が指摘されている。

本年度の活動として当委員会は、クラウド/SaaS 時代において、情報セキュリティ対策のニーズがどのようになるか、JEITA 会員企業にとってどの様なビジネス展開が期待できるかを明らかにすることを目的として調査を行った。調査内容としては、(1) クラウド/SaaS 関連市場・技術・参入プレイヤなどの動向調査、(2) 米国のクラウド/SaaS 主要事業者動向調査、(3) クラウド/SaaS 時代の情報セキュリティ製品・サービス利用状況・意向調査を専門家の講演受講、サービス提供企業へのヒアリング、ユーザ企業に対するアンケート調査などを通じて行い、その結果を、報告書としてとりまとめた。

本調査報告書の作成にあたり、視察やアンケートにご協力いただいた企業やご講演いただいた関係者の方々、そして当委員会の関係の皆様に深く感謝の意を表すとともに、本報告書が関係の方々に活用され、今後のセキュリティビジネスのさらなる発展に寄与できれば幸いである。

2010 年 3 月

セキュリティ市場・技術調査専門委員会

委員長　遠藤　淳

セキュリティ市場・技術調査専門委員会名簿

（敬称略・順不同）

委員長	遠藤　淳	三菱電機㈱
副委員長	福島孝文	東芝テック㈱
委員	伊藤　丘	コニカミノルタビジネステクノロジーズ㈱
〃	角田光弘	㈱日立製作所
〃	池田政弘	富士ゼロックス㈱
〃	池田恵一	富士通㈱
〃	白石節男	富士通㈱
〃	畠山有子	三菱電機㈱
〃	平木博史	㈱リコー
オブザーバ	村瀬一郎	㈱三菱総合研究所
〃	川口修司	㈱三菱総合研究所
〃	江連三香	㈱三菱総合研究所
〃	丸田佳織	㈱三菱総合研究所
事務局	佐野眞一	（社）電子情報技術産業協会
〃	吉田　晃	（社）電子情報技術産業協会

目　次

1. クラウド/SaaS 市場動向

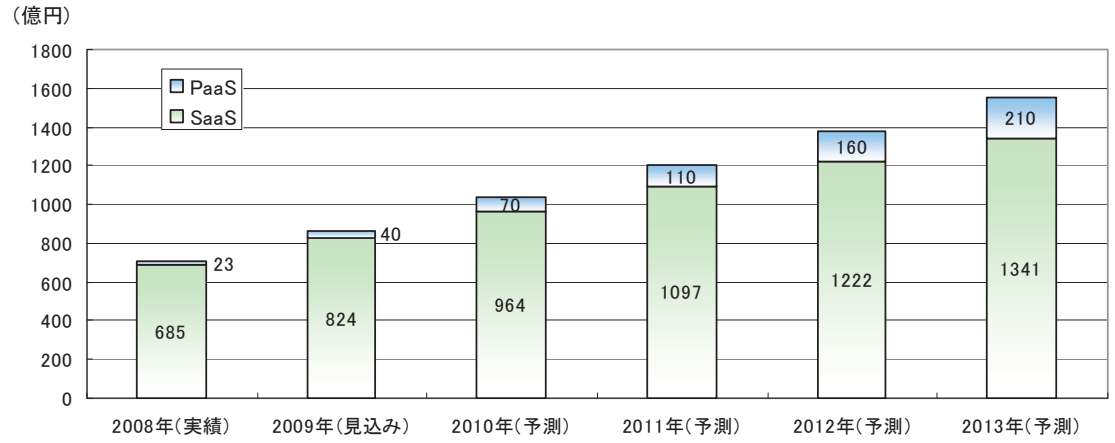
1. 1. 市場動向

1. 1. 1. 国内市場動向

(1)概況

高速・安価なネットワーク環境の普及、Web 技術の進展、米国における Amazon や Salesforce.com の台頭などにより、1999 年頃登場した“ASP サービス”の形態はクラウド/SaaS として注目され始め、国内におけるクラウド/SaaS 環境も、大手 IT ベンダなどがクラウド事業への参入を表明するなど、ここ数年、市場として急速に立ち上がりを見せ始めている。

国内における市場規模の展望は、図 1.1.1-1 に示す通り、着実な拡大傾向を示している。



出典：富士キメラ総研、『2009 年 SaaS/PaaS 関連市場の現状と将来展望』

図 1.1.1-1　SaaS/PaaS 関連サービス市場規模推移/予測（2008 年度～2013 年度）

SaaS 市場においては、2008 年度実績（685 億円）と比較して、

・2009 年度見込み（824 億円）　　：120%の伸長率

・2013 年度予測（1,341 億円）　：約 2 倍の成長

また、PaaS 市場においては、2008 年度実績（23 億円）と比較して、

・2009 年度見込み（40 億円）　：174%の伸長率

・2013 年度予測（210 億円）　　：約 9 倍の成長

と示されるように市場拡大が予測されており、今後数年での急速な普及拡大が見込まれる。

今後、ユーザ企業における初期投資圧縮の傾向が強まった場合や、本格的に PaaS が活用されサービス事業者の参入が増加した場合は、ユーザ企業における SaaS 利用の拡大、さらなる市場規模の拡大の可能性もあると思われる。

(2)国内主要ベンダ・SIer、サービス事業者等の動向

米国内の市場が Amazon（2006 年 8 月）、Salesforce.com（2007 年 7 月）などのサービス提供開始により急速に立ち上がっていく中で、日本国内におけるクラウド/SaaS 市場の立ち上がりは遅れていたが、2009 年頃より富士通・NEC・日立製作所などの大手 IT ベンダ、NTT データなどの SIer、KDDI などの大手 ISP などが軒並み事業戦略を発表し、国内でもいよいよクラウド/SaaS 時代の到来となった。

国内大手ベンダ・SIer 各社においては、これまでのシステムインテグレーションで培ったノウハウをクラウドコンピューティング関連のサービスとして展開し、主にプライベート・クラウド構築支援に主軸を置き、事業推進している状況にある。

例えば、富士通では、2009 年 10 月より、クラウドサービス基盤としてシステムリソース、ネットワーク、セキュリティ、マネジメントサービスからなる大規模仮想化プラットフォーム「Trusted-Service Platform」の提供を開始するとともに、クラウド導入にあたっての対象業務の見える化、最適化、既存システムとの連携などトータルなサポートを推進している。

また、日立製作所では、2009 年 7 月より、クラウド関連のサービスを、ビジネス PaaS ソリューション、ビジネス SaaS ソリューション、プライベート・クラウドソリューションから構成される「Harmonious Cloud」として新たに体系化し、クラウドの導入コンサルテーションから設計、構築、運用まで、トータルなサポートを提供している。

国内大手ベンダ・SIer 各社では、データセンターの維持費が海外と比較して高額であることなどから、先行する外資系クラウド/SaaS 事業者に対して価格面での競争力を持つことが困難であることもあり、顧客対応でシステム開発を行ってきた従来のビジネスの延長線上にクラウド/SaaS ビジネスを位置づけていると考えられる。ひとつのサービスモデルに特化してサービス提供を行うのではなく、ユーザ企業が懸念する信頼性・セキュリティなど技術面での優位性や、導入前のコンサルテーションから稼動後の運用までトータルなサポートが可能である点を強調し、ユーザ企業への囲い込みを図っていると見られる[1]。

一方、国内のサービス事業者においては、2007 年頃より、ネットワーク環境の普及を背景に、従来提供していたサービスを中心に SaaS 型として提供を始めるケースが見られるようになった。

本委員会の現地調査[2]で伺った「株式会社 HARP」「札幌市 SaaS ビジネス研究会」の事例においても、電子申請・電子調達・施設予約の SaaS での提供が既にされている他、教育機関向けや士業向け等サービス提供に関するビジネス検討が進められている。

SaaS 型の事業展開においては、バックエンドなどの独自仕様の強い部分ではなく、まずはフロント系の共通化が図りやすい部分から普及していく見通しであり、そういった点で

[1] 各社のクラウド/SaaS 事業展開の概要は、本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」1.2.2 参照。
[2] 本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」付録Ⅱ 講演録参照。

も、事業者の取り組みとしては“連合体”に向けたサービス展開から着手・検討されている状況と言える。

(3)国内におけるクラウド/SaaS ビジネス環境の特徴

クラウドコンピューティングのサービスモデルとしては、大きくいうと、パブリック・クラウド、プライベート・クラウドに分けられる。

米国 Amazon などがパブリック・クラウドによるサービスモデルを展開し、利用が拡大しているのに対し、日本国内のユーザ企業においては、社内システムのクラウドへの移行は、全体としてまだ慎重な姿勢をとっている状況と言える。

この背景には、

- 企業内のデータを社外に保管（特に海外のデータセンター）することに対して日本企業が抵抗感を持つこと
- 品質や信頼性、セキュリティ等に対して日本企業が敏感になる傾向があること
- 日本企業においては大手ベンダ・SIer への依存度が高い傾向があること

などが挙げられる。

このため、国内企業のクラウド/SaaS の利用においては、主にプライベート・クラウドとして構築する形態、または、業務によってプライベート・クラウドとパブリック・クラウドを使い分けるハイブリッド・クラウドで構築する形態が現実的と見られている。

こういったクラウドサービスの導入に際しては、プライベート・クラウド・パブリック・クラウド両方に対して、連携やマネジメント環境の構築の必要性、オンプレミスで稼動する既存システムとクラウドの連携環境構築の必要性が出てくるため、今後、“クラウド・インテグレーション”のニーズが出てくるものと想定され、国内ベンダ・SIer 各社では新たなビジネスモデルを模索している段階でもある。

今後のユーザ企業でのクラウド普及とともに、ソフトウェアベンダ、ハードウェアベンダ、SIer、ISP 事業者などの間で、付加価値要素や棲分け、差別化も明確になってくると想定される。

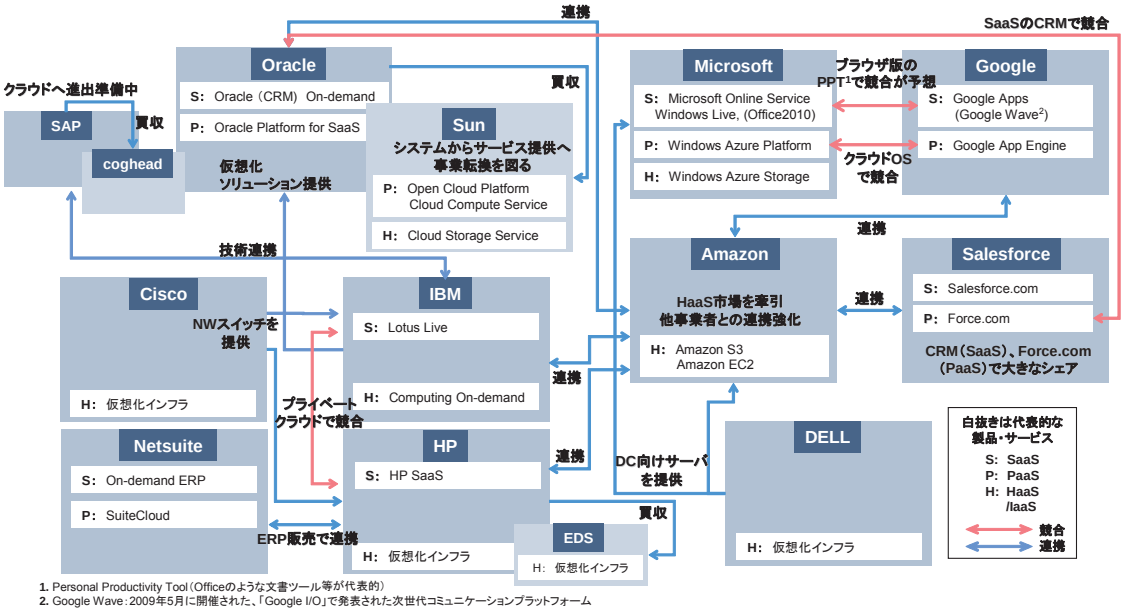
1. 1. 2. 米国市場動向

(1)米国の主要クラウド/SaaS 事業者の動向

米国においては、ソフトウェア、ハードウェア或いは各種サービスのベンダである様々な企業が、自ら保有する優位な技術や資産をコアにして、クラウドビジネス市場へ次々に参入し、展開を進めている。

例えば、Amazon は、世界最大規模に数えられるウェブサイト（Amazon.com）のインフラを基盤として、Amazon Web Services（以下 AWS）と呼ばれるサービスをインターネット経由で提供しつつ、パブリック・クラウドの環境整備を急速に進めている。また、IBM は、世界最大規模に数えられる IT サービス企業として、基本的なインフラ、ミドルウェアから利用可能な幅広いサービスに至るまで、クラウド・コンピューティングサービスにおける全般的な価値連鎖を提供し、主にはプライベート・クラウドの展開に注力している。

米国のクラウド業界での連携と競合動向を図 1.1.2-1 に示すが、Google や Salesforce 等が先行する中、既存のハードウェアベンダもクラウド向け製品や、クラウド事業者へのインフラ提供に力を入れている。一方で既存ソフトウェアベンダもクラウド技術を持つ企業を買収するなどして、自社製品のクラウド転換に向けた準備を進めている状況にある。



出典：週刊ダイヤモンド（2009 年 5 月 16 日号）、各社公表資料、報道等を基に三菱総合研究所作成

図 1.1.2-1　米国のクラウド業界動向[3]

[3] 代表的事業者の動向概要は、本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」第 2 章を参照。

(2)米国のクラウド普及の特徴

米国においては、クラウド普及が日本よりも先行しているが、その特徴は、日本市場と比較すると以下の通りである。

- 主要なクラウド/SaaS 事業者の世界的な台頭（Amazon、Salesforce.com など）
- 中小企業におけるクラウド利用の進展
- パブリック・クラウドに対する市場ニーズの増大

その背景として、米国における次のような IT 市場の特徴が挙げられる。

- 米国ではユーザ側の情報システム部門に製品・サービス導入に関する選定能力があるが、日本においてはベンダ側が主導して選定する傾向が強い。
- ユーザ側の業務の標準化が進んでおり、IT サービスにおける共通化が容易である。
- インターネット・ネットワーク技術に強く、最新技術やノウハウが入手出来る。

米国は、クラウドサービスを提供するための基幹技術である、データセンター用のサーバや高速スイッチ、合理化システムなどの点で世界をリードしており、さらに、将来的にも、データセンター間でアプリケーションや情報処理能力などをやり取りするために一層複雑で高度なノウハウが必要になっていくことが予想され、米国のクラウドサービス分野での技術的な優位性は暫く揺るがないものと思われる。

1. 2. クラウド/SaaS におけるセキュリティ

クラウド/SaaS におけるセキュリティについて、米国国立標準技術研究所（NIST: National Institute of Standards and Technology）のクラウドセキュリティの分析を参照する[4]。クラウドの重要事項として信頼性、マルチテナント、暗号化、コンプライアンスを挙げており利点と課題がある。一般的なクラウドセキュリティの利点としては　①外部のクラウドに公開データを移すことによる内部機密データの露出低減、②クラウドの同質性によるセキュリティの監査/テストの簡易化、③セキュリティ管理の自動化、④冗長性/災害復旧、がある。また、一般的なクラウドセキュリティ上の課題としては、①ベンダのセキュリティモデルを信頼すること、②監査結果に顧客が対応出来ないこと、③調査のための支援が必要、④間接的な管理者の責任、⑤独自の実装ができない、⑥物理的な制御ができない等がある。

クラウド/SaaS の活用が先行している米国では多くの業界団体が設立されている。特にクラウド/SaaS のセキュリティに関する検討を行う Cloud Security Alliance が公表したガイドライン「Guidance for Critical Areas of Focus in Cloud Computing」はクラウド事業者及び組織のセキュリティ担当者向けに作成された文書で、組織内で「適切なガバナンス」「リスクマネジメント」「常識」を維持することが重要とし、クラウドセキュリティのベストプラクティスとして作成している。「クラウド・アーキテクチャ」、「クラウドにおけるガバナンス」、「クラウドにおけるオペレーション」の 3 章 13 ドメインで構成されており、各ドメインについて事業者とユーザに向けた推奨事項が示されている。

クラウド/SaaS 事業者のユーザに対するセキュリティ確保のアカウンタビリティは、従来から顧客と取り交わされているサービス品質保証契約（Service Level Agreement：以下、SLA）に記載してお互いに確認しているケースが多い。一般に、SLA ではサービスの範囲やサービスの品質を評価する指標、指標に基づく品質の目標値などを取り決めるが、セキュリティについても同様な考えで、個別ユーザ毎に異なるニーズに合わせてまとめられている。実際の運用におけるセキュリティ確保は現時点では各社各様であり、外部のセキュリティ事業者に一部を委ねたり、或いは、全てを自前で対応する等で対策が打たれている。

例えば、Amazon では AWS インフラにおけるデータの完全性は最終的に顧客側に責任がある。そこで、顧客におけるセキュリティへの懸念に対応するために、自身の AWS フレームワークに加え、セキュリティサービスを提供する複数のソリューションプロバイダと協業している。

また、IBM では自社のクラウドサービスにおける各局面を網羅した SLA によって、顧客へのアカウンタビリティを保持している。顧客が懸念するクラウドコンピューティングでのセキュリティ関連問題を把握した上で、自社の IBM Security Framework やその他の自社のセキュリティ製品（外部のパートナーに殆ど依存する必要が無い）を利用して対応している。

---

[4] NIST, “Effectively and Securely Using the Cloud Computing Paradigm v26”, http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

国内における取り組みとしては、2008 年頃より経済産業省及び総務省を中心にクラウド/SaaS に関する技術、法制度等の検討が活発に行われており、それらの活動の中でもセキュリティの確保が重要な観点として扱われている。

利用促進のためのガイドラインとして経済産業省が作成した、SaaS 利用者向けの「SaaS 向け SLA ガイドライン」[5]はセキュリティに関して、①公的認証取得の要件、②アプリケーションに対する第三者評価、③情報取扱者の制限、④情報取扱い環境、⑤通信の暗号レベルを取り上げている。他にも ASP/SaaS 事業者における情報セキュリティ対策促進のための「ASP・SaaS における情報セキュリティ対策ガイドライン」が制定されている。

業界団体でもサービス提供者側からの「クラウドサービスプロバイダ協会」や異なる事業者間の相互運用性を目指した「クラウド・ビジネス・アライアンス」が設立されている。

国内の多くの企業がクラウド/SaaS の導入の障害としてセキュリティ確保を課題としている。その中で、国内で早くからサービスを展開している Salesforce.com 社では、機密性、保全性、可用性に加えて、監査性を含めた 4 つのセキュリティ対策を行い、顧客の不安に応えるだけでなく、規模の経済を利用した高度なセキュリティレベルをメリットとして打ち出して実績を上げている[6]。

これらの調査検討から、クラウド/SaaS におけるセキュリティ確保の主な課題として以下の 4 点が挙げられる。①データの取扱い（機密性）、②コンプライアンス・監査（監査性）、③相互運用性・移植性（可用性/完全性）、④事業継続性・インシデント対応（可用性/完全性）である。これらの課題に明確な対応法を示すことでクラウド/SaaS が日本企業でも活用されることに繋がると考えられる。

国内大手ベンダ・SIer 各社においては前節で紹介したように、これまでのシステムインテグレーションで培ったノウハウをクラウドコンピューティング関連のサービスとして展開し、トータルなサポートを推進している。品質やセキュリティに敏感な傾向のある顧客に対しプライベート・クラウドやハイブリット・クラウドが中心に普及が進むと考えられる。

また、国内で提供されているクラウド/SaaS のセキュリティサービスは従来のパッケージ製品を SaaS に移行させたものが大半であり、プレイヤも既存事業者が多いが、SaaS 市場からの参入事業者も増えており今度の動向が注目されている。

主なセキュリティサービスとしては、ウィルス対策、ログ収集・管理及び IT 資産管理サービスなどで、右肩上がりの伸びが予想されている。（以下、市場予測は国内トータル市場）

ウィルス対策は最も一般的なセキュリティツールであり、かつウィルス定義ファイルの更新がサーバによって一元化されるため、従来のパッケージ製品に比べユーザやマシンの負担が軽減されるというメリットがある。2008 年度実績は 24 億円、2013 年度には 43 億円

[5] 経済産業省「SaaS 向け SLA ガイドライン」
http://www.meti.go.jp/press/20080121004/03_guide_line_set.pdf
[6] 本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」付録Ⅱ 講演録参照。

の市場規模[7]が予測されている。

ログ収集・管理は J-SOX 法で注目を集め、2008 年度実績で 3.25 億円、2013 年度には 15 億円の市場規模が予測されている。今後は PCIDSS（Payment Card Industry Data Security Standard）対策としても期待されている。

IT 資産管理はクライアント PC の管理支援やセキュリティ対策を行うサービスである。ログ収集・管理と同様に J-SOX 法によってニーズが高まっているが、導入企業は大企業が中心である。IT 資産管理の SaaS 市場はパッケージベンダから、エンジン提供を受けて参入している事業者が多く、2008 年頃から新規事業者が増加している。2008 年度実績で 0.9 億円、2013 年度には 11 億円の市場規模が予測されている[8]。

[7] Web セキュリティやメール対策ソリューションは対象外。

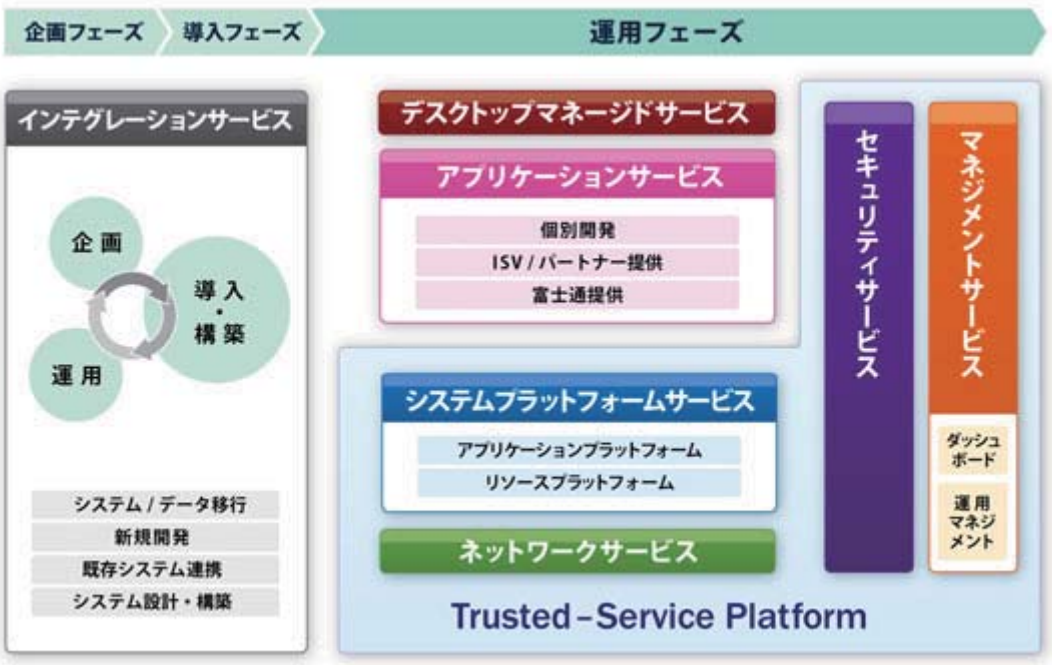
[8] クラウド/SaaS におけるセキュリティ関連製品・サービスの動向は、本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」1.3.3 節を参照。

1. 3. 委員企業の取り組み

ここでは、委員企業のクラウド/SaaS の主な取り組みを紹介する。

1. 3. 1. 富士通

富士通では、2009 年 4 月にクラウドサービスに関する発表を行い、順次サービスの提供を進めている。企画・導入から運用までの全てのフェーズで、必要なプラットフォームとサービスをワンストップで提供している。クラウドサービスの核となるのが、クラウドサービス基盤「Trusted-Service Platform」（以下、TSP）である。TSP は、クラウドコンピューティング時代に向けて、信頼性・セキュリティ・可用性・拡張性・省エネルギーを高いレベルで実現する大規模仮想化プラットフォームである。TSP に加え、クラウド導入にあたっての対象業務の見える化、最適化、既存システムとの連携など、お客様の ICT システムをトータルにサポートする。



出典：富士通

図 1.3.1-1　富士通のクラウドサービス体系[9]

(1)企画・導入フェーズ

① インテグレーションサービス

クラウド環境を利用する業務システムと企業内で構築・運用する業務システムの

[9] 富士通, クラウドコンピューティング・クラウドサービス
http://fenics.fujitsu.com/outsourcingservice/cloud/services/index.html

切り分けなど、業務プロセスの可視化を行いながら適用方法についてコンサルティング、具体的なインテグレーションを実施。

(2)運用フェーズ

① デスクトップマネージドサービス
お客様が業務で使われるデスクトップ環境を、シンクライアントやモバイル環境、メール・グループウェア等の OA ツールも含めて提供。

② ネットワークサービス
利用者を把握し、多様な端末・アクセス回線を活用して安心・安全に企業内ネットワークに接続。

③ セキュリティサービス
データセンター内のクラウド環境における情報資産の保護の徹底と資産の正当性維持等のセキュリティガバナンス確立を支援。

④ マネジメントサービス
クラウドサービスとして提供する各機能を統合的にマネジメントするサービス。システムリソース/ネットワーク/アプリケーションの稼動・運用状況、セキュリティ状況、消費電力/CO_2 排出量等を可視化する。

⑤ システムプラットフォームサービス
サーバ、ストレージ、OS、ミドルウェア等を仮想的な資源として管理し、お客様の要望に応じて必要資源を提供。

⑥ アプリケーションサービス
データセンターから提供される最先端のアプリケーション機能を、必要なときに必要なだけ利用できる SaaS アプリケーションサービス。

これら各サービスの提供にあたり重視しているのが、セキュリティと品質である。これまで培ってきたコンピューティング技術・ネットワーク技術・運用管理の技術、ノウハウを結集し、お客様が安心して利用できる、セキュアで信頼性の高いクラウドサービスの提供を目指している。また、他社のクラウドサービスとも連携し、お客様にとって最適なクラウド環境の提供も進めている。

1. 3. 2. 日立製作所

日立製作所のクラウド/SaaS への取り組み事例を紹介する。

日立では、コスト削減や導入スピード、柔軟性といったクラウドサービスの持つ良い点に加えて、高信頼、高セキュリティで環境にも配慮した日立クラウドソリューション「Harmonious Cloud（ハーモニアスクラウド)」（以下、HC）の提供を 2009 年 7 月に開始し、導入時のコンサルテーションから設計、構築、運用までをトータルに提供している。

出典：日立製作所

図 1.3.2-1　日立製作所のクラウドサービス体系[10]

(1)サービスの特長

日立のクラウドサービスの特徴として、以下の点が挙げられる。

① 高信頼

電力・交通・金融システムといったミッションクリティカルな企業情報システムにも適用できる高信頼なクラウドコンピューティング環境を実現。

② 高セキュリティ

ネットワークでは、ネットワークパーティションによるユーザ専用のネットワーク環境を、サーバでは日立独自の仮想化技術である日立サーバ仮想化機構「Virtage」のハードウェアによる仮想化アシスト機能を、ストレージでは独立した仮想論理ユニットを割り当てることができ、クラウド環境においても、従来のコア業務システムと同等の高セキュリティを実現。

[10] 日立製作所, クラウドソリューション「Harmonious Cloud」
http://www.hitachi.co.jp/products/it/harmonious/cloud/

③　環境配慮

先進のグリーン IT 技術を駆使した環境配慮型データセンターを軸に、省電力運用技術を結集したサーバ、ミドルウェア、ストレージなどにより、環境配慮型のクラウドコンピューティング・プラットフォームを実現。

(2)提供ソリューション

現在 HC では、以下のソリューションを提供している。

表 1.3.2-1　HC の提供ソリューション

ソリューション名	内　　容
ビジネス PaaS ソリューション	企業での利用に必要な水準の信頼性・セキュリティを備えた IT プラットフォームリソース（PaaS）を提供し、コストや導入時間を短縮する、HC の核となるソリューション
ビジネス SaaS ソリューション	自社で IT システムの構築/運用をしたくない業務アプリケーションをネットサービス形態（SaaS）で利用し、標準的な業務機能を低コスト、短期間で導入するソリューション
プライベート・クラウドソリューション	顧客のサイト内に、プライベート・クラウド（IT リソースプール）を構築するソリューション

1. 3. 3. リコー

リコーのクラウド/SaaS への取り組み事例を紹介する。

リコーは、2009 年より日本 IBM と提携し、同社の情報共有ソフトウェア「IBM Lotus Notes／Domino」の機能をネットワーク経由で提供するなど、ビジネスに役立つソフトウェア機能をクラウド環境で利用する複数のサービスを提供している。

(1)サービスの特徴

リコーのクラウドサービスの特徴として、以下の点が挙げられる。

① 迅速なサービス利用
自社でサーバ環境を持つ必要がなく、初期投資を抑え、契約からシステム利用開始までの期間を短縮することが可能となる。

② 運用コストの軽減
サーバ管理・運用の手間から解放され、システムの運用負荷が大幅に軽減される。

③ サポート提供
コールセンターによる問い合わせ対応などのサポートを提供する。

(2)提供サービス

現在リコーでは以下のサービスをクラウドサービスとして提供している。

表 1.3.3-1 リコーの提供サービス[11]

サービス名	内　　容
RICOH Cloud for Lotus Notes/Domino	Lotus Notes/Domino を月額利用で提供し、リコーグループの社内実践で培ったノウハウを活かし運用負荷軽減、投資コスト低減、事業継続への対応を実現可能にする。
eCalendarOffice	インターネットを通じてオフィスの情報共有を実現する ASP 型グループウェアサービス。スケジューラ・設備予約など便利な機能を搭載。携帯電話、PDA などのモバイル端末にも対応する。
NetRICOH α-MAIL	独自ドメインを提供する簡単・便利なホスティングサービス。電子メール機能・ホームページ機能を提供する。
salesforce.com	営業支援（SFA）・マーケティング支援・サービス&サポート支援、代理店管理（PRM）などの機能を持ち、顧客・商談の情報をデータベース上で一元管理する顧客管理サービス。部門をまたいで企業全体での情報共有や業務効率向上（営業活動やマーケティング活動の生産性向上など）を実現する。

[11] リコー, クラウドサービス
http://www.ricoh.co.jp/outsourcing/cloud/

NETBegin Web 会議システム	定額で安心の ASP 型 Web 会議サービス。日本全国、インターネット環境があれば会議に参加可能となる。

また、コンシューマー向けの Web サービス「quanp（クオンプ）」[12]を 2008 年 5 月 12 日から開始している。「quanp」は、デジタルカメラで撮影した画像やビデオ映像、パソコンで作成した文書、さらに音楽ファイルなどの様々な情報を、Web 上にアップロードしたり、共有できるオンラインストレージサービスである。

「quanp」の特徴として、

① 最大 100GB の大容量で様々なファイルを保存可能
② 優れた検索機能
③ ユーザを指定したファイル共有機能
④ 使いやすく直感的操作にこだわったユーザインタフェース
⑤ 写真、動画、文書までサムネイル表示に加え、キーワード検索
⑥ デスクトップに飾れるスライドショーやオンラインプリント等
⑦ 自社開発、自社運用で高いセキュリティ

などがあげられる。

[12] リコー, quanp
http://www.quanp.com

1. 3. 4. 富士ゼロックス

富士ゼロックスでは、2002 年 10 月より複数のネットワークサービスを提供している。

(1)beat：ネットワークアウトソーシングサービスを介して提供されるサービス群

beat によって提供されるサービス群の特徴として、以下が挙げられる。

① 強固なセキュリティ対策の提供
サービス専用のアプライアンスサーバ「beat-box」が、インターネットの出入口で不正アクセス、ウィルスなど、様々なインターネットの脅威から社内 LAN 全体を防御するため、配下にある PC も統一されたセキュリティ強度で守られる。

② 運用コストの軽減
「beat-box」の管理を含めて、ネットワークサービスの運用管理をセンターで一括に行なうため、システムの運用負荷が大幅に軽減される。

③ サポート提供
コールセンターによる問い合わせ対応により、ネットワークサービスの利用サポートを行う。

ネットワークサービスとしてのサービスメニューは、以下の通りである。

表 1.3.4-1　富士ゼロックスのネットワークサービス

サービス名	内容
Working Portal	中小規模事業所のお客様向けに、IT 利活用の促進と、業務効率化を支援する社内用のポータルサイトとして 2010 年 2 月より提供開始[13]している。
文書ストレージサービス	beat-box で暗号化し、たがいに 100km 以上離れた 3 ヶ所のデータセンターに同じ文書を記録することで災害時の文書喪失リスクを分散する。データセンター容量 1GB の文書ストレージ機能は beat サービスの標準機能として提供され、オプションサービスとしてデータセンター容量 3, 5, 10, 20, 50GB 拡張がある。
サイボウズ ASP サービス	サイボウズ®[14]を ASP としてご提供する有償オプションサービスを提供している。
ケータイリモートサービス	携帯電話で外出先や出張先からオフィス内の情報を共有し、スピーディな業務遂行、業務の効率化を支援するサービスとして提供している。

[13] 当初は地域限定の 300 社へ提供。
[14] 現在は、サイボウズ® Office 8 を提供。

モバイルメールサービス	リモートメール[15]を利用して時間や場所を選ばずに、オフィスの届くメールを携帯電話で閲覧・返信できるサービスとして提供している。

(2) Knowledge-Drive：動画を含むドキュメント配信・アウトソーシングサービス

中・大手企業向けを対象とした、動画を含むドキュメント配信の ASP サービスをベースに、業務アウトソーシングサービスとして提供している。サービスの特徴は下記の通りである。

① ASP サービスとアウトソーシングメニューの組合せ
動画配信の ASP サービスとともに、お客様のコンテンツ流通業務プロセスにおける「前工程（収録業務、コンテンツ作成、メディア変換)」、「後工程（コンテンツの登録、保管、配信役務代行)」といったアウトソーシングメニューから、お客様のご要望に沿って組合せて提供する。
② 問い合わせ、業務代行の受付も含む、一括したサポート窓口。
③ インターネット間での動画配信機能

[15] リモートメールは株式会社 fonfun が提供するサービス。

2. クラウド/ SaaS 時代の情報セキュリティ対策ニーズの状況

2. 1. 調査方法の概要

クラウド/ SaaS 利用におけるセキュリティに関する課題、セキュリティ確保のポイントの明確化、クラウド/ SaaS 時代における情報セキュリティ市場性を把握するため、日本のユーザ企業におけるクラウド/SaaS の利用動向、さらにクラウド/SaaS を利用している企業における導入方法や、利用における管理方法等を調査した。日本企業全体における利用動向を把握し、同時に実際の利用者の状況を深く探るため、本調査は 2 段階のウェブアンケート調査で実施し、第 1 次調査では、社内担当者に対して社内のクラウド/SaaS 利用の有無、利用意向を聞き、第 2 次調査では第 1 次調査においてクラウド/SaaS を利用している或いは利用を検討していると回答したモニタを対象に、詳細な利用状況を聞いた[16]。

2. 2. 調査結果

第 1 次調査では 2,403 名の回答者に対して、クラウド/SaaS の利用動向について調査を行った。現在クラウドを「利用している」と回答した割合は 22.1%、また「現在利用していないが、今後利用を検討している」と回答した割合は 23.1%となり、半数近くが、クラウド/SaaS 利用に対して積極的な姿勢を見せている。一方で「現在利用しておらず、今後も利用する予定はない」（39.4%）と回答した回答者にその理由を聞いたところ、「必要性がない」との回答が 68.8%を占めた。なお「セキュリティに不安がある」との回答は 19.5%であった。

日本企業における現在のクラウド/SaaS の利用は、比較的導入に積極的な企業と、そもそもの必要性を感じないため、検討も行わない企業とに 2 極化している状況がある。

第 2 次調査では、第 1 次調査においてネットワーク上のサービスを「利用している」または、「現在利用していないが、今後利用を検討している」と回答した 305 名に対してサービス別の利用状況・利用意向を調査し、さらに「利用している」と回答した 152 名に対して、詳細な利用状況を調査した。

クラウド/SaaS 利用者の内、基幹系のみを利用しているのは、12.5%、非基幹系のみを利用しているのは 37.5%となり、両方を利用しているのは 50.0%であった。さらに従業員数が 300 名以下の規模の小さい企業では、特に非基幹系のみの利用（51.0%）が目立ち、企業規模が大きくなるに従い基幹系の利用が進んでいる。

本調査結果によって明らかになった点を以下にまとめる。

[16] 本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」第 3 章及び付録 III 参照。

(1) クラウド/SaaS の利用状況

回答者の企業におけるクラウド/SaaS 利用率は 2 割強、利用検討率も 2 割強であり、今後も一定の割合まで普及が進むと考えられる。

またシステム別には、非基幹系/基幹系とも大企業における利用が先行しており、中小企業ではグループウェアやメールといった特定サービスの利用に限定されている。

(2) クラウド/SaaS の利用形態

非基幹系のみを利用している企業では、外部のクラウド環境を利用する割合が高いのに対し、基幹系を利用している企業では自社内に構築したクラウド環境を利用する割合が高くなっている。本調査における「自社内のクラウド環境」は純粋な「プライベート・クラウド」を指すものではない可能性があるが、基幹系はプライベート・クラウド、非基幹系はパブリック・クラウドという一定の切り分けがなされていると考えられる。

また、基幹系利用者に絞って分析を行った結果、基幹系を外部環境、つまりパブリック・クラウドで利用する企業では、自社内環境で利用する企業に比べてデータを外に出すことへの不安が大きい傾向が見られた。

(3) クラウドに求めるメリット

クラウド/SaaS を利用することで得られるメリットはコスト削減効果との回答が圧倒的に多く、サービス内容やセキュリティ面では未だ事業者側のメリットに繋がっていない状況が伺える。一方で、特に大企業においてクラウド/SaaS 事業者の選定において、サービス内容、価格に次いでセキュリティ対策が重視されているという結果が得られた。事業者側にとっては、クラウド/SaaS のサービスにおいてセキュリティ面でどの様な付加価値を出せるかが課題となっている。

(4) クラウド/SaaS におけるセキュリティへの不安

利用者が感じるセキュリティ上の課題として、最も多く挙げられたのが、「データが社外に保管される」、「サービスがインターネット上に公開される」という点であった。クラウドにおけるセキュリティ上の課題としてデータの取扱いが頻繁に議論されている通り、ユーザ側の不安もこの点に集中している。

またセキュリティ確保を重視している回答者は、「クラウド/SaaS 専業者の従業員によるミス、内部不正」、「直接監査が実施出来ない」といったコンプライアンスや監査等、技術面以外での不安も聞かれた。

(5)利用者が求めるセキュリティサービス

クラウド/SaaS 導入時に既存システムからの移行に苦労したと回答した回答者では「既存システムも含めた全体システムに対するセキュリティサービス」へのニーズが高く、セキュリティ確保に苦労したと回答した回答者では「クラウド/SaaS のプラットフォームにおけるセキュリティへの第 3 者評価」へのニーズが高くなった。また基幹系システム利用者からは「クラウド/SaaS 導入支援」に対するニーズも高く、各社が利用するクラウド/SaaS の形態と利用状況によって様々なサービスが求められている。

2. 3. 情報セキュリティ製品・サービス導入状況

ここでは、クラウド/SaaS 利用動向とは別に毎年実施している情報セキュリティ製品・サービス導入実態と利用動向調査の結果を紹介する。

本年度の導入率が高いサービスは、メールフィルタリングツール・サービス（53.9%）、データバックアップツール（55.2%）、Web アプリケーションファイアウォール（48.3%）であった。なお、本年度はウィルス対策ツールやファイアウォール等、既に導入率が非常に高く、経年の変化が見られない製品・サービスは調査対象から除外し、比較的導入率が変化している製品・サービスに絞って調査を行った。

経年変化として 2007 年から 2009 年まで比較した場合は、シングルサインオン、メールフィルタリング等のサービスは 2007 年段階では導入過渡期であったが、本年度の調査においては大企業において大半の企業で導入が進み、また中小・中堅企業でも徐々に導入/導入検討が進んでいる様子が窺える。また、シンクライアントに関しては、例年導入検討率が高い傾向にあるが、導入率が大きく増加することはないため、企業が導入に踏み切れない状況があると考えられる。

3. クラウド/SaaS 時代における日本の情報セキュリティ産業

3. 1. 日本のクラウド/SaaS の今後

日本における SaaS/ASP の導入傾向は近年急速に高まっている。日経マーケット・アクセスの調査によると、SaaS/ASP を現在使用しているとした事例における「使用開始時期」は、「2007 年 4 月以後」が約半数を占めたとのことである。このことは、ここ数年の SaaS ブーム期に様子を見ていた企業が実際に導入を開始することによって、事例数が急増していることを示していると見ることができる。

その背景には、「運用・メンテナンスコスト・期間の削減」、「システム開発コストの削減」、「ハードウェアコストの削減」といった、クラウド/SaaS 活用のメリットが評価され、導入に踏み切る傾向が高まっていることが挙げられる[17]。また、自社でシステム構築を行うことなく、システムを所有せずに利用することによる TCO 削減効果を企業が望むのと平行して、高速ネットワーク・インフラの普及、仮想化技術の進歩、クラウド/SaaS 事業者の相次ぐサービス提供開始などの技術革新が進むことによって導入の負荷が低減され、利用するクラウド/SaaS の選択肢が増えたことも、この傾向を後押ししているものと思われる。

一方で、導入に至らない要因として「カスタマイズを重要視する特殊性」と「信頼性・セキュリティに対する不安」が主たる要因として挙げられている。前者に関しては、システムの所有を前提として独自仕様を是とする日本特有の企業文化や価値観に起因している。そのため、業務プロセスの分解と標準・汎用機能を用いた再定義を行う改革の負担と導入のメリットとのトレードオフで判断されてゆくものと考えられる。

ここで言う日本特有の企業文化や価値観とは、システム構築において独自性を追求するためにカスタマイズを行うという特徴や、システムを構成するハードウェアやアプリケーションソフトウェアを所有する傾向を指す。独自性の追求は標準的なパッケージソフトの適用によるコストメリットの理解が進むことにより緩和され、所有へのこだわりも所有・維持するための費用とサービス利用料の比較により変化してゆくであろう。

後者に関しては、「データが社外に保管される」、「サービスがインターネット上に公開される」、「クラウド/SaaS 事業者の従業員によるミス、内部不正の可能性がある」などの理由が具体的な懸念事項として示されている[18]。これらの課題に関しては、クラウドの利用形態の多様化によるセキュリティ強化が進むものと想定される。

---

[17] 本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」図表 3-12 参照。

[18] 本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」図表 3-18 参照。

クラウドの利用形態については、下記のパターンに分類される[19]。

- パブリック・クラウド
  インターネットから到達可能であり、不特定多数の企業・利用者からアクセスされるクラウド環境で稼動する SaaS を活用する。
- ハイブリッド・クラウド
  インターネットから到達可能であり、不特定多数の企業・利用者からアクセスされるクラウド環境で稼動する SaaS と特定企業に限定してアクセス可能に設定されたクラウド環境で稼動する SaaS を併用する。
- プライベート・クラウド
  特定企業に限定してアクセス可能に設定されたクラウド環境で稼動する SaaS のみを利用する。

企業のシステムの多くを基幹系システムで占める企業以外、すなわち大多数の企業は何らかの形態でパブリック・クラウドを活用することが予想される。そのため、パブリック・クラウドのセキュリティを強化するような商品・サービスの提供が、今後の日本におけるクラウド/SaaS 普及の鍵を握るものと思われる。

国内のクラウド/SaaS 事業者だけでなく、欧米で成功事例として繰り返し紹介されているクラウド/SaaS 事業者が日本にその拠点を立ち上げてサービスを提供するなどの事例も見られるようになった。このような傾向は、海外にデータを預けることに不安を持つ企業の懸念を払拭するとともに、導入の選択肢をさらに広げることになる。こうした対応の積み重ねによって、導入のメリットが導入の不安を凌駕したとき、さらなるクラウド/SaaS の普及が見られることが予想される。

これらに加えて、既に提供されているクラウド/SaaS のセキュリティを強化するサービスが出現したり、クラウド/SaaS 事業者のセキュリティを評価して格付けするような動きも始まっている。こうした動きは、セキュリティを強化したいクラウド/SaaS 事業者とその利用者双方にとってメリットをもたらすと同時に、セキュリティを確保するための課題と対策、そして複数のクラウド/SaaS 事業者と利用者の間での責任分界点に関する議論を促進するであろう。

[19] 本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」図表 4-1 参照。

3. 2. クラウド/SaaS 時代における日本の情報セキュリティ産業の方向性

日本におけるクラウド/SaaS の利用形態に、パブリック・クラウド、プライベート・クラウド、ハイブリッド・クラウドの 3 形態があることは、前節で示した通りである。大企業、中小企業を問わず業務システムでセキュリティを確保することは重要事項である。

クラウド/SaaS 利用者の望んでいるセキュリティサービスは「既存システムも含めた全体システムの対するセキュリティサービス」と「クラウド/SaaS プラットフォームにおけるセキュリティへの第三者評価」であることがわかった[20]。

つまり､クラウド/SaaS を利用することで業務システム全体のセキュリティが確保でき、そのセキュリティ機能が市場で要求されているセキュリティ基準を満足している事を証明するセキュリティサービスをクラウド/SaaS 利用者は望んでいるということである。

セキュリティサービスのビジネス展開においてどの様な方向性があるのかを、クラウド/SaaS の普及に伴うセキュリティの在り方の変化、そしてそれに伴う市場構造の変化の予測から考えると表 3.2-1 の様になる。

表 3.2-1　セキュリティサービスの展開とビジネス性

ビジネス展開		サービス提供先	ビジネス性
①	エンドユーザに対する新たなセキュリティサービスの提供	エンドユーザ（クラウド/SaaS利用者）	△
②	クラウド/SaaS事業者に対する専門セキュリティサービス	クラウド/SaaS事業者	×
③	セキュリティサービスのクラウド/SaaS化	クラウド/SaaS事業者及びエンドユーザ	○
④	複数のクラウド/SaaS事業者を束ねたクラウド・インテグレーション	クラウド/SaaS事業者及びエンドユーザ	◎（※）

※主として大手SIer／ベンダが事業中心となる
◎：とても有望　　○：有望　　△：やや有望　　×：有望でない

これらの大きな違いは、セキュリティサービスビジネスを「クラウド/SaaS 事業者」「エンドユーザ（クラウド/SaaS 利用者)」のどちらに向けて提供していくのか（①、②)、或いは自らがセキュリティサービスを展開して両社に提供していくのか（③、④）ということである。

クラウド/SaaS 事業者やエンドユーザ（クラウド/SaaS 利用者）をターゲットとしたセキュリティサービスは、セキュリティベンダ各社が既に保有している製品群やサービス群をクラウド/SaaS 環境に展開するビジネスとなる。このため、新規参入は難しいと考えられ

[20] 本篇付録（株）三菱総研「クラウド/SaaS 時代のセキュリティ技術と関連ビジネスに関する調査」図表 4-3 参照。

る。従って、新規にクラウド/SaaS でセキュリティビジネスを立ち上げる場合においてはビジネス展開③、または④のどちらかが有望と考えられる。

ビジネス展開③の「セキュリティサービスのクラウド/SaaS 化」では、クラウド/SaaS 環境で必要なセキュリティ技術やセキュリティ管理技術を利用者の要望に対応したサービスメニューとして提供すればよいので、比較的容易に、中小事業者でもセキュリティサービスをクラウド/SaaS で展開することが可能となる。また、セキュリティサービスは標準化することで、クラウド/SaaS システムの信頼性を確保することと、セキュリティ機能を第三者に評価してもらうことが可能となる。このことは、標準的なセキュリティ機能を中小企業でも低コストに導入できることを示しており、日本の企業全体のセキュリティレベルを向上させるのにも有効である。クラウド/SaaS 利用者の要望を常に聴き、信頼や安心を確保し提供を続けることがサービス事業者にとって必要である。しかし事業参入が比較的容易であるために、事業者間の競争が激しくなりコスト競争になる可能性もある。このために提供するセキュリティサービスに大きな特徴を持つことが重要になる。

ビジネス展開④の「複数のクラウド/SaaS 事業者を束ねたクラウド・インテグレーション」では、パブリック・クラウドとハイブリッド・クラウドの環境下で、全体システムの最適化と全体システムのセキュリティを確保するサービスの提供することになり、今後の最も有望なセキュリティビジネスである。しかし、システム利用形態が多様化するに伴い、複数のクラウド/SaaS 事業者を束ねたクラウド・インテグレーションのインタフェースをとることと、利用者のセキュリティポリシーにあったセキュリティ機能を提供する必要があり、その対応は大手ベンダや SIer にしかできない領域であると言える。

次に、利用者視点からどの様なビジネス展開を持つクラウド/SaaS 事業者が必要になるのかを、プライベート・クラウド、パブリック・クラウドについて考える。

プライベート・クラウドは、企業内或いは業界内に閉じたクラウド/SaaS の利用になるので、利用する企業や業界のセキュリティポリシーに従ったクラウド/SaaS 環境に対応したセキュリティ関連製品やサービスを選定して利用すればよい。つまり、主に「ビジネス展開①、②の事業者」を活用することになる。

パブリック・クラウドを利用する多くの中小企業はクラウド/SaaS が提供するセキュリティ機能を利用して標準的なセキュリティを低コストで業務システムにすぐに組み込みたいという要望を持っている。つまり、「ビジネス展開③の事業者」を中心に活用する。これにより、セキュリティ意識の強い大企業だけでなく、中小企業でもセキュリティレベルを向上させることが可能となる。しかし、中小企業の利用者にとっては過大なセキュリティ機能の提供や運用を強いられ、かえって業務効率の低下や運用コストの増大を招くなどの恐れもある。また、事業内容によってはさらなるセキュリティレベルの向上を要求することも考えられる。このためサービスメニューをカスタマイズできるサービス事業者を利用する必要がある。

パブリック・クラウドを利用して事業を構築する最大のメリットは前節で述べている通り「コストの削減」である。また、どんなに優れたサービスであっても、100%完全なもの

は存在しない。今後も様々なクラウド/SaaS が提供され、さらなるコストの削減や、事業に適したサービスが登場することも十分に予測される。このため、利用しているクラウド/SaaS を別のクラウド/SaaS に乗り換えることも視野に入れる必要がある。クラウド/SaaS の乗り換え時には今まで利用していたクラウド/SaaS が提供するセキュリティ機能やサービスも容易に移行できる仕組みが必要になる。このクラウド/SaaS の乗り換えを考えた場合に有望なセキュリティサービス事業者としては「ビジネス展開④の事業者」を活用するのが良い。つまり、複数のクラウド/SaaS 事業者とセキュリティ連携をとりながら、利用者の業務内容やセキュリティポリシーにあったセキュリティ機能を提供するセキュリティサービスの利用である。これは、クラウド/SaaS サービスを仲介するサービスを利用することとも言える。このサービスを利用することで、利用者のセキュリティレベルを全く変更することなく、クラウド/SaaS の乗り換えも容易に可能となる。また、クラウド/SaaS 事業者から見ると、業界や事業内容によって異なる利用者のセキュリティポリシーは意識しなくてもセキュリティ仲介サービス事業者に任せておけば良いので、新規業界分野へとクラウド/SaaS サービスを展開できるといったメリットがある。このため、ビジネス展開④「複数のクラウド/SaaS 事業者を束ねたクラウド・インテグレーション」が最も有望なビジネス形態である。このビジネス形態は、先に述べたように、このビジネスは大手事業者や SIer にしかできないものである。しかし、業界毎のセキュリティ機能の提供は中小事業者でも可能であるので、大手ベンダや SIer と連携をとって業界固有のセキュリティ機能を提供してセキュリティインタフェースを構築するなどのビジネス展開も考えられる。（図 3.2-1）

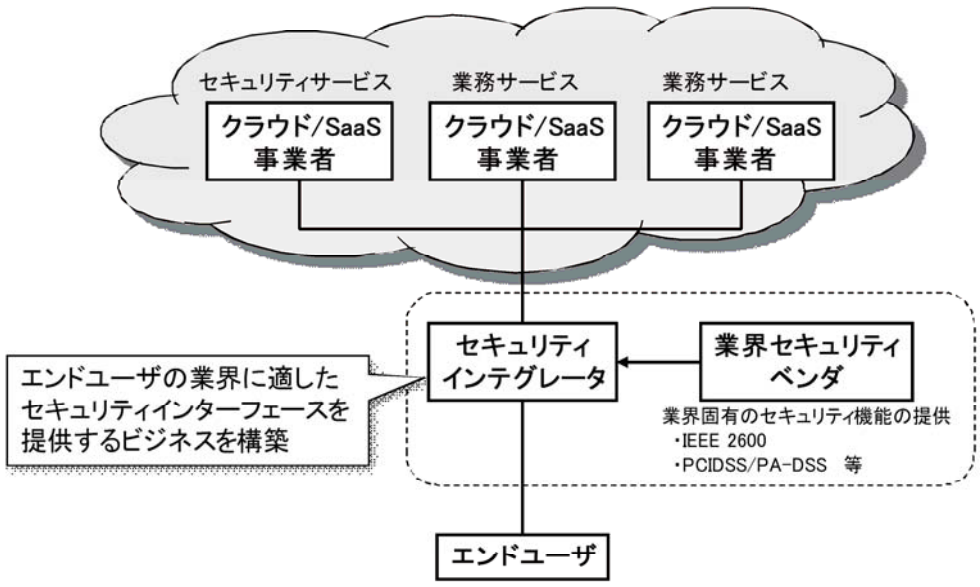


図 3.2-1　クラウド/SaaS で有望なセキュリティビジネス形態

クラウド/SaaS 時代は、汎用的に提供されるクラウド/SaaS を事業内容や業務にあわせて必要なサービスを選択し利用することで、業務システム構築にかかる時間や費用などのコストを削減することが大きな目的である。このため、クラウド/SaaS 利用者はクラウド/SaaS サービスの変更や追加する毎に新たなセキュリティ技術や管理策を導入することはコスト面から避けたいと考えている。従って、セキュリティサービスをクラウド/SaaS で提供する事業者はどの様なクラウド/SaaS でも利用でき、信頼性が高い利用者インタフェースを構築することが必要となってくる。

また、利便性のために、一人の利用者が PC、携帯電話、携帯端末などの複数のデバイスを使って同じクラウド/SaaS にアクセスすることも考えられるので、今後は PC 以外のデバイスを利用してもセキュリティを確保ながらクラウド/SaaS を利用できるようなセキュリティサービスが必要になってくる。

クラウド/SaaS 時代のセキュリティ産業のあるべき姿は、複数のパブリック・クラウドを、多くのアクセス・デバイスを利用しても、クラウド/SaaS を利用する企業のセキュリティポリシーを満足するセキュリティサービスを低コストで提供することにある。多くの場合、業界毎に標準的なセキュリティポリシーが策定されていることが多いので、セキュリティサービス事業者はそれぞれの業界に適したセキュリティ機能を提供して既存システムにも導入していくことが必要となる。これにより業務システム全体のセキュリティを確保することが可能となる。また、クラウド/SaaS のシステムが正常に機能していてセキュリティが確保されていることが利用者で確認できるような機能や、クラウド/SaaS システム自体も第三者評価を実施するなどし、サービス利用者の信頼を確保していかなければならない。これにより、利用者のセキュリティ機能に対する要望を満足することができるのである。

日本におけるクラウド/SaaS の第三者評価には、「特定非営利活動法人 ASP・SaaS インダストリコンソーシアム（ASPIC）」[21]が設けている「ASP・SaaS 安全・信頼性情報開示認定制度」がある。また、そのクラウド/SaaS システムで ISO/IEC15408（Common Criteria）等の評価認証を取得することも、クラウド/SaaS 利用者の信頼を得るために効果的である。

[21] ASPIC, http://www.aspicjapan.org/

おわりに

本年度の調査にて、クラウド/SaaS 時代における情報セキュリティビジネスの方向性として、複数のクラウド/SaaS 事業者を束ねたクラウド・インテグレーション、プライベート・クラウド、パブリック・クラウドを含めたユーザのシステム全体のセキュリティ評価、クライアントセキュリティの確保、またはそれを含めたシステム全体のセキュリティ確保のビジネスが有望となってくるとの結論に達した。このようなビジネス形成により、会員企業のみならず多くの企業において、クラウド/SaaS を安全に、安心して利用できる環境が整い、クラウド/SaaS の普及とともに、情報セキュリティ産業が発展していくことを期待する。

クラウド／SaaS 時代のセキュリティ技術と関連ビジネスに関する調査

平成２２年３月

株式会社三菱総合研究所

目次

序章　調査の概要

0.1. 調査の背景と目的

ストレージコストの低減や分散処理技術の高度化、通信環境の充実など、安価な ICT 基盤が急速に整いつつある昨今、「クラウド・コンピューティング」のサービスに注目が集まっている。クラウド・コンピューティングとは、ユーザがインターネット上（クラウド＝雲）に分散するコンピューティング機能を利用するモデルである。クラウド・コンピューティングにおいては、ユーザは最低限の接続環境（クライアント端末、ブラウザ、インターネット接続環境）があれば、インターネット上のサーバ群が提供する多様なアプリケーションやデータストレージを「サービス」として利用することができる。現在、米国の Google、Amazon、Salesforce.com などがクラウドサービスの代表的な事業者である。

クラウドは、ソフトウェアをインターネット経由で提供する「SaaS（Software as a Service）」「ASP（Application Service Provider）」を包含する概念として位置づけられる。本調査では、これらのサービスを「クラウド/SaaS」と呼ぶ。

クラウド/SaaS は、ユーザにおける ICT の導入や運用の負担を抑制するソリューションとされる。特に、IT 予算や IT 人材の確保が困難な中小企業には極めて有効なモデルとして期待されており、経済産業省では中小企業の IT 利活用を促進する施策として 2009 年 3 月 31 日から中小企業向け SaaS 活用基盤（J-SaaS）の運用を開始した。その一方で、クラウド/SaaS はビジネスやミッション・クリティカルな業務に適さないという見方もあり、国内における普及シナリオは未だ明確ではない。加えて、自社データがインターネット上のどこに保管されているかわからないという不安もあり、安全性や信頼性（SLA：Service Level Agreement）、適法性（アウトソーシングに対する個人情報保護法、J-SOX の要請、業界別の規制など）をどのように担保するかという課題が指摘されている。

さらに、クラウド/SaaS は、従来の ICT 業界の産業構造を大きく変革する可能性があることから、クラウド/SaaS 時代のセキュリティのビジネスモデルの在り方について研究し、その対応を検討することが重要である。

そこで、本調査では、以下の項目について明らかにすることを目指す。

- クラウド/SaaS 市場動向（日米の比較、有望マーケット、将来展望等）
- セキュリティビジネスに与える影響
- JEITA 会員企業におけるセキュリティビジネス戦略の方向

0.2. 調査の視点

0.2.1. 本調査における定義

本調査においては、クラウド及びSaaSを以下のように定義し、両者を含む形でクラウド/SaaSと表現する。

クラウド・コンピューティング（Cloud Computing）： クラウド・コンピューティングを指すものとし、サーバ等が提供するサービスを、リソースを意識せずにネットワークを通じて使用できるモデルと定義する。SaaS（Software as a Service）やPaaS（Platform as a Service）等を包含したより広い概念。
SaaS（Software as a Service）： ユーザ側のコンピュータがソフトウェアを保有するのではなく、ソフトウェアの機能をサービスプロバイダがネットワークを通じて提供するモデルと定義する。ASP（Application Service Provider）の進化形で、利用者にとってより使い勝手がよく、利用価値が向上したものとする。

0.2.2. 本調査の視点

クラウド/SaaSが普及することで、日本企業においてもアプリケーションやインフラの「所有」から「利用」への流れが加速化し、従来のハードウェア/ソフトウェアの調達、システムインテグレーション等の市場ニーズが低下することが予想される。

但し、日本企業では従来カスタマイズされたシステムが主流であるため、クラウド/SaaSへの単純な移行は難しいと考えられる。また企業の情報セキュリティに対する意識が高く、情報を外に出すことを警戒する風潮があるため、クラウド/SaaSの考え方が素直に受け入れられない可能性がある。さらに、情報システム系、Web系等のクラウド/SaaSへの親和性の高い分野と基幹系システム等の移行が難しい分野があるため、すべてのシステムをクラウド/SaaSに移行させることは現実的でない。

そこで本調査においては、日本におけるクラウド/SaaS普及によるシステムインテグレーションに影響ある分野を特定し、分野毎・ターゲット毎のセキュリティビジネスの動向予測を行う。

0.3. 調査フロー

本調査は以下に示すフローに従って実施する。主な調査内容を以下に示す。

(1) クラウド/ SaaS の概念を整理し、関連する近年の市場・技術、クラウド/SaaS ビジネスへの参入プレイヤ等、クラウド/SaaS に関連する動向の調査を行い、情報セキュリティ市場に影響を与える要素を整理する。

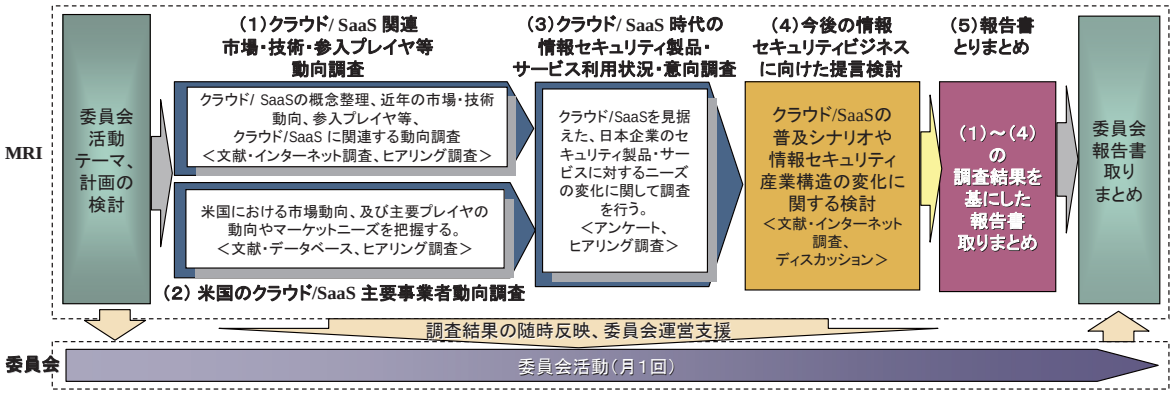
(2) クラウド/SaaS ビジネスが先行する米国における、情報セキュリティ市場に影響を与えるプレイヤの動向やマーケットニーズを把握し、今後の日本におけるセキュリティビジネス動向を予測するための示唆を得る。

(3) 日本のユーザ企業におけるクラウド/SaaS の導入意向やセキュリティ製品・サービスに対するニーズの変化に関して調査を行い、情報セキュリティ製品・サービスに対する国内ユーザのニーズをターゲット毎に明確化する。

(4) クラウド/SaaS の普及シナリオを踏まえた上で今後の情報セキュリティ産業構造の変化について検討し、JEITA 会員企業として今後の情報セキュリティビジネスの可能性を検討する。

(5) 以上の調査結果を基に、報告書の取りまとめを行う。

図表 0-1-1　本調査のフロー



第 1 章　クラウド/SaaS 関連市場・技術・参入プレイヤ等動向調査

1.1. クラウド/ SaaS ビジネスの動向

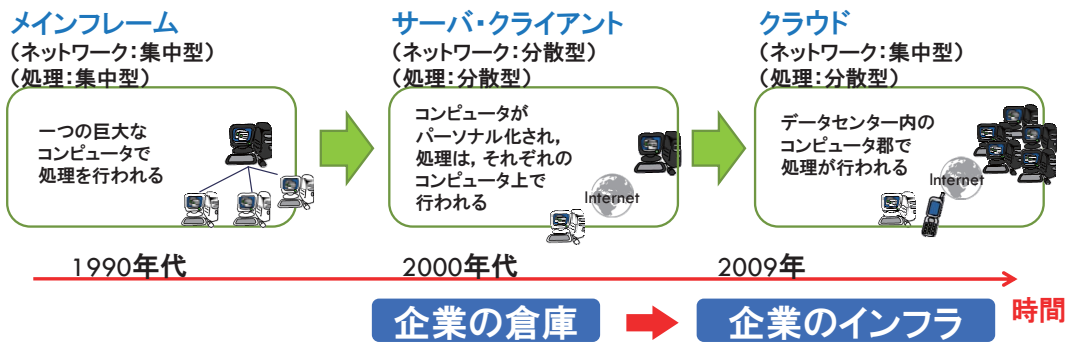
1.1.1. クラウド/SaaS 普及の背景

(1) IT 産業の構造変化と企業の IT 資産に関する状況の変化

昨今のクラウド/SaaS 普及の背景の 1 つには 2000 年代後半に入ってからの IT 産業の構造変化がある。企業システムのプラットフォームにおける変化で言えば、1990 年代におけるメインフレームの集中型のネットワーク及び処理から、2000 年代はサーバ・クライアントへの分散型ネットワーク及び処理、そしてここ数年は集中型ネットワーク上で分散処理を行ういわゆるクラウド型のプラットフォームへと変化してきている。

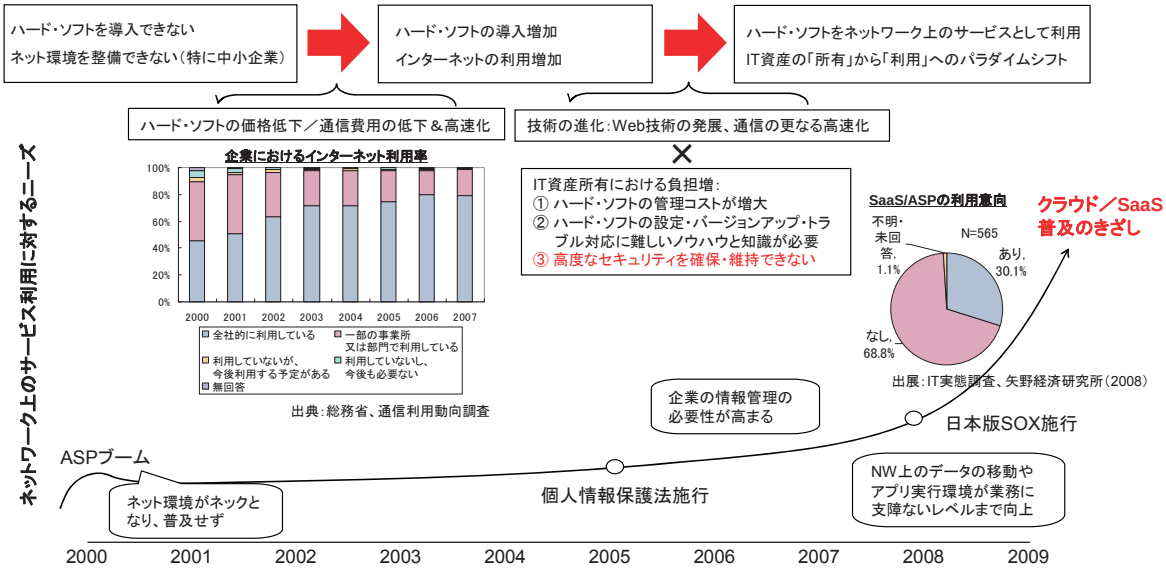
また、企業の IT 資産に関する状況も大きく変化している。IT 化の進展に伴い、企業が所有するハードウェアやソフトウェアの IT 資産は年々増加してきたが、同時にそれらに課される管理及び各種の法制度等の制約により企業の IT 資産所有にかかる企業側の負担も増加してきた。企業側が IT 資産を「所有」せずに、ネットワーク上のサービスを「利用」するという考えは、1999 年頃に登場した ASP（Application Service Provider）という形でも提唱されてきた。ASP は当初一時的にブームを迎えたものの、当時の通信環境において顧客に対して安価で安定したサービスを提供することは難しく、大きな市場形成には至らなかった。しかし、近年のネットワークの高速化と各種の Web 技術の進展によって、ASP で提唱されたサービスの形が、クラウド/SaaS という形で再度脚光を浴び、Amazon や Salesforce.com といった米国の事業者の登場により急速に市場が拡大してきている。事業者が米国中心であることから、日本企業におけるクラウド/SaaS の普及は遅れていたが、2008 年後半頃より日本の事業者もクラウド/SaaS への参入を相次いで表明しており、今後国内市場の拡大が期待される。

図表 1-1　プラットフォームの変化



資料：三菱総合研究所作成

図表 1-2　企業の IT 資産に関する状況の変化



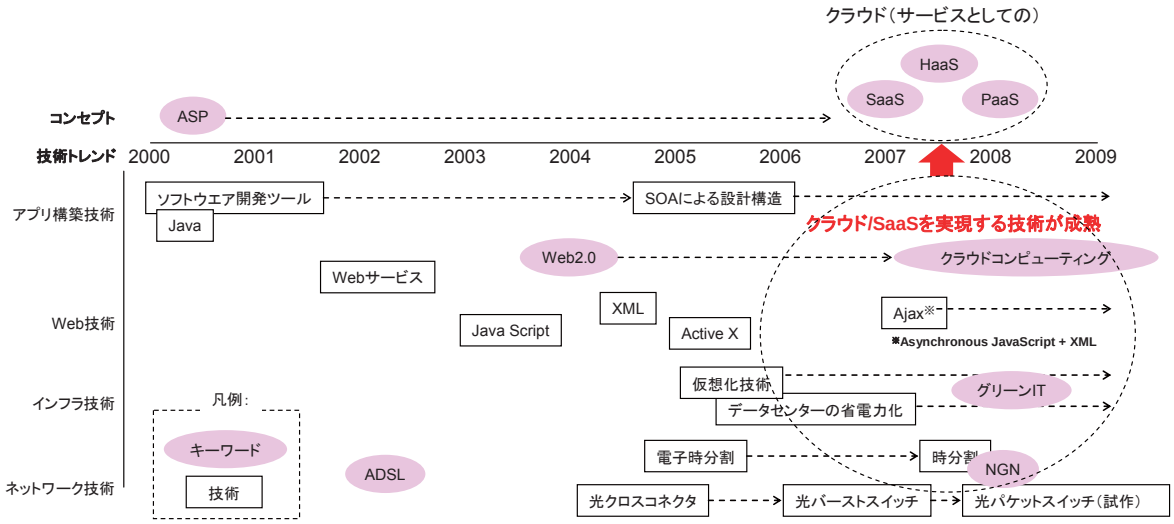
資料：総務省、ASP・SaaS の普及促進策に関する調査研究を基に三菱総合研究所作成

(2) クラウド/SaaS を実現する技術の発展

「クラウド」や「SaaS」は特定の技術を指すものではなく、IT、ネットワークに関わる様々な技術を複合的な形で利用するサービスの形態を指すものである。クラウド/SaaS には 2000 年代後半に開発されたネットワーク技術や Web 技術等が多く利用されている。クラウド/SaaS を実現する技術の例を以下に示す。

- ネットワーク技術：NGN 関連技術
- インフラ技術：仮想化技術、クラスタ技術、分散処理技術（Amazon や Google 等の巨大データセンター運用ノウハウ）
- Web 技術：Web サービス、XML、Ajax
- アプリ構築技術：サービス指向アーキテクチャ（Service Oriented Architecture）
- その他：サービス基盤技術、クライアント端末の性能向上

図表 1-3　クラウド/SaaS を実現する技術



資料：情報処理学会誌 2008 年 11 月号「ASP・SaaS の動向と普及促進の状況」を基に三菱総合研究所作成

1.1.2. クラウド/SaaS の概念整理

本調査におけるクラウド/SaaS の定義は、0.2.1. に示した通りだが、ここでは米国国立標準技術研究所（NIST: National Institute of Standards and Technology）が公表しているクラウド・コンピューティングの定義を参照しつつ、クラウド/SaaS の概念を体系的に整理する。

クラウド・コンピューティングは「クラウド（雲）」という表現の通り、インターネット（雲）を介して、雲のあちら側のリソース（サーバ等）を意識することなく、サービスを利用出来る環境及び技術を指す。クラウド・コンピューティングの定義は数多くあるが、現在最も参照される定義は、以下に示す NIST の定義である。

NIST におけるクラウド・コンピューティングの定義（翻訳は IPA 資料参照）[1, 2]

“*model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*”

「（複数のユーザにより）共有され、（最適環境を）設定・調整可能なコンピューティング資源に、簡易かつオンデマンド・ベースでネットワークからのアクセスが可能な形態（モデル）のこと。当該コンピューティング資源は最小限の管理能力やプロバイダの関与だけで、迅速に提供され、解除される。」

[1] NIST, http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

[2] IPA（NIST 文書の翻訳）, http://www.ipa.go.jp/about/NYreport/200909.pdf

クラウド/SaaS の特徴として、一般的には仮想化技術により実現されるリソースの抽象性や弾力性が挙げられるが、NIST における定義ではサービス自体の在り方やデバイスの観点も含め、以下の 5 つの点で整理されている。

クラウド・コンピューティングの特徴

- On-demand self-service:
  消費者（ユーザ）は、サービスプロバイダの人的関与を必要とせず、自動的に、一方的にコンピューティング能力（サーバやネットワークストレージ）を利用出来る。
- Broad network access:
  コンピューティング能力は、各種の消費者のプラットフォーム（携帯やラップトップ、PDA など）から、ネットワークを通じてサービスや資源にアクセスできる。
- Resource pooling:
  プロバイダのコンピューティング資源は、Multiple-Tenant モデルにより、複数の消費者に提供され、その物理的・仮想的資源は消費者の需要に応じて動的に割り当てられる。その際、消費者は、一時的に、どこで計算がなされるか、管理できず知見を有さないという点で、場所に独立的である。
- Rapid elasticity:
  コンピューティング能力は、急速かつ弾力的に、スケールイン・スケールアウトされて、提供される。消費者から見ると、コンピューティング能力は無限であるように見え、必要な時に必要な量を購入することができる。
- Measured Service:
  クラウドシステムは、計算能力を利用することにより、サービスのレベルに応じて、資源利用の管理・最適化が自動的に行われる。資源の利用は、プロバイダ、ユーザの両方にとって、監視、制御され、透明性を以て報告される。

また、クラウド・コンピューティングのサービスモデルとして、以下の 3 つのモデルが挙げられる。本調査における「SaaS」もクラウド・コンピューティングの 1 つのサービスモデルと捉えることとする。

クラウド・コンピューティングのサービスモデル

- SaaS（Software as a Service）:
  ユーザが、プロバイダがクラウド・インフラ上で提供するアプリケーションを、利用出来るようなコンピューティング能力。アプリケーションは、クライアントの各種デバイスによってアクセスできる。
- PaaS（Platform as a Service）:
  ユーザが、プロバイダが提供するプログラミング言語・ツールを用いて、消費者自らがクラウド・インフラ上で開発・購入したアプリケーションを利用出来るようなコ

ンピューティング能力。

- IaaS（Infrastructure as a Service）または HaaS（Hardware as a Service）:
  ユーザが、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）を利用し、任意のソフトウェア（OS やアプリケーションを含む）を利用することができるような能力。

クラウド・コンピューティングの導入モデルは、以下の 4 つに分類される。本調査においては、主にパブリック・クラウドとプライベート・クラウド、またその複合形としてのハイブリッド・クラウドに焦点を当てる。

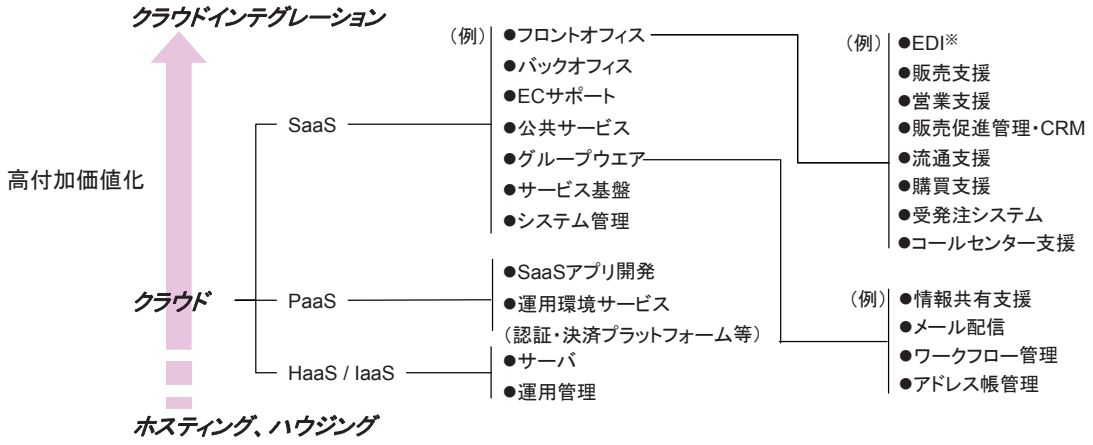
クラウド・コンピューティングの導入モデル

- パブリック・クラウド:
  クラウド・インフラが、一般国民や大きな産業グループによって利用されるものであり、クラウドサービスを提供する 1 つの組織によって提供されるもの。
- プライベート・クラウド
  クラウド・インフラが、一組織によって運営されているもの。第三者によって管理されている場合もあり、また、敷地内/敷地外の場合がある。
- コミュニティ・クラウド
  クラウド・インフラが、複数の組織によって共有され、共通意識（ミッション、セキュリティ要件、政策、コンプライアンス等）を有する特定のコミュニティによって支援されているもの。第三者によって管理されている場合もあり、また敷地内/敷地外の場合がある。
- ハイブリッド・クラウド
  クラウド・インフラが、2 つ以上のクラウド（プライベート、コミュニティ、パブリックなど）からなるとともに、データやアプリケーションの移動を可能にする規格または占有の技術により、1 つの統一されたクラウドとして利用されるもの。

1.1.3. サービスとしてのクラウド/SaaS の分類

現在、市場では図表 1-4 に示すように SaaS、PaaS、HaaS/IaaS において様々なサービスが存在する。各市場における競合も年々高まってきており、サービス内容の高付加価値化が重視されている。従来、ホスティングやハウジングといった場所貸しに近いサービスであった国内のクラウド/SaaS 事業は、様々な形態のサービスを提供する現在の形へと進化してきている。さらに今後はクラウド/SaaS に、コンサルティング等を組み合わせ、企業のシステム全体を最適化するクラウド・インテグレーションという新たなサービス形態も生まれつつある。

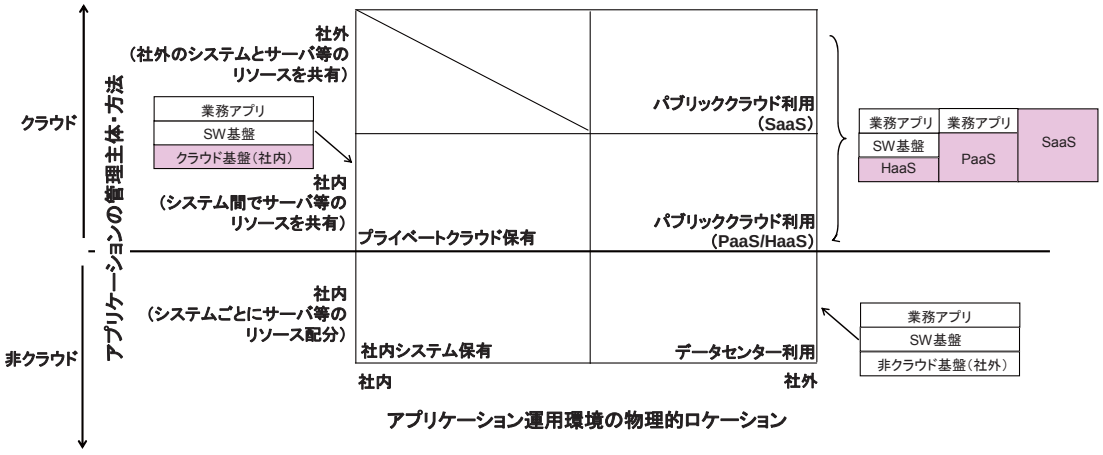
図表 1-4　クラウド/SaaS として提供されるサービスの例



資料：三菱総合研究所作成

従来の社内システムやデータセンターはシステムの物理的ロケーションは異なるが、どちらもシステム毎にサーバ等のリソースが割り当てられるという点で共通している。一方、クラウドではサーバ等のリソース（基盤）をシステム間で共有している点に特徴がある。事業所を多く抱える大企業では、イントラネット上に散らばるサーバを仮想化し、企業専用のクラウド基盤とすることで、プライベート・クラウドを構築することも可能である。

図表 1-5　クラウド/SaaS の分類



資料：新日鉄ソリューションズの資料[3]を基に三菱総合研究所作成

[3] 新日鉄ソリューションズ、http://www.ns-sol.co.jp/casestudy/pdf/nssol-te-prir-doc-005-01.pdf

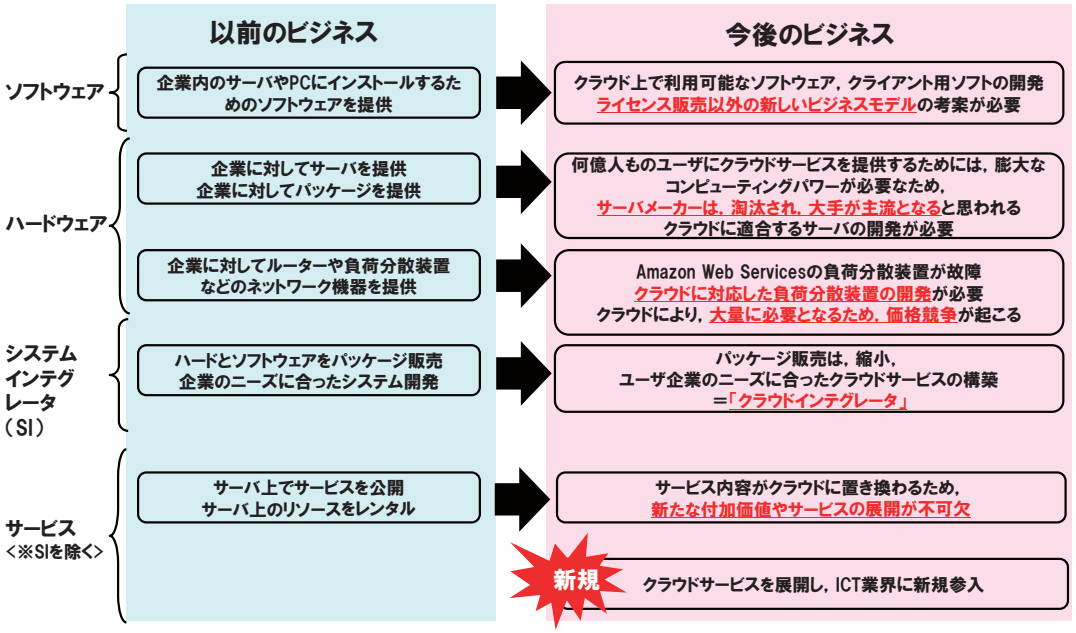
1.1.4. クラウド/SaaS におけるビジネスの変化

市場で先行するクラウド/SaaS 事業者が新規ユーザの獲得や事業者間の連携を強化しさらなるサービス拡大を図る一方で、IT の既存プレイヤはそのビジネスの在り方に変革が求められている。

既存のソフトウェア/ハードウェアベンダは既存サービスにクラウド/SaaS の要素を加えることで、一部ビジネスモデルの転換を図る動きが見られる。また、従来の SIer は、企業の要望に応じてクラウド/SaaS を含めた企業の IT 環境を構築することが必要となり、その結果としてクラウド・インテグレーションという新たなビジネスモデルが生まれている。クラウド・インテグレーションの主な中身としては、クラウド環境における企業のシステム開発及びその支援、各種クラウド/SaaS のサービス連携等が挙げられる。特にカスタマイズされたシステムを多く有する日本企業の場合、システムすべてをクラウドに移行することは現実的でないため、オンプレミスで稼働する既存システムとクラウドに移行したサービスとの連携におけるニーズが最も高くなると考えられる。しかし、クラウド/SaaS 導入の大きな目的の 1 つがコスト削減であることから、クラウド・インテグレーションの規模は従来のシステム・インテグレーションより縮小されることが予想され、国内の SIer はクラウド/SaaS 環境における新たなビジネスモデルを模索している段階である。

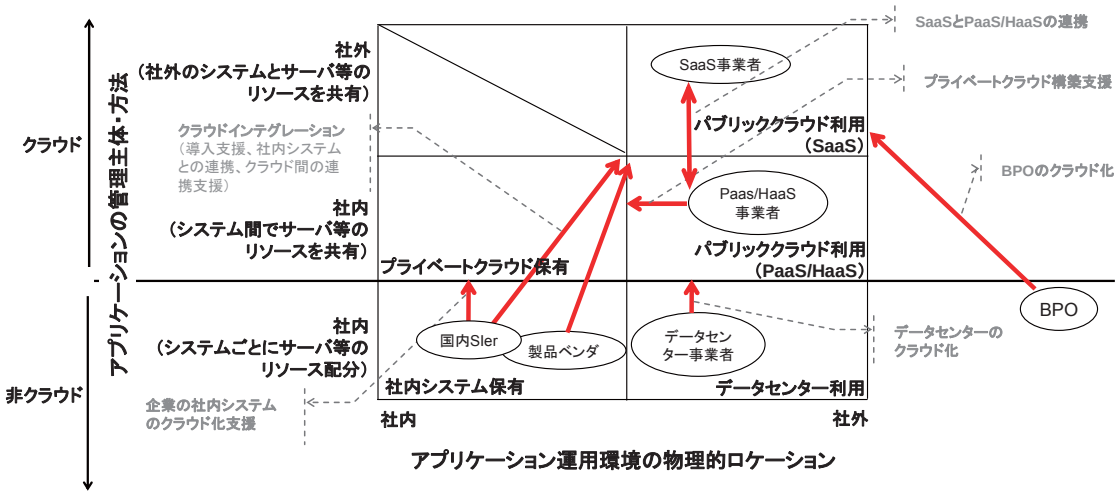
いずれのプレイヤも、先行する事業者との差別化を明確にするため、提供するサービスにどのような付加価値を出せるかが重要となっている。

図表 1-6　各プレイヤのビジネスの変化



資料：三菱総合研究所作成

図表 1-7　各プレイヤのビジネスフィールドの変化



資料：新日鉄ソリューションズの資料[4]を基に三菱総合研究所作成

1.2. クラウド/ SaaS 市場の動向

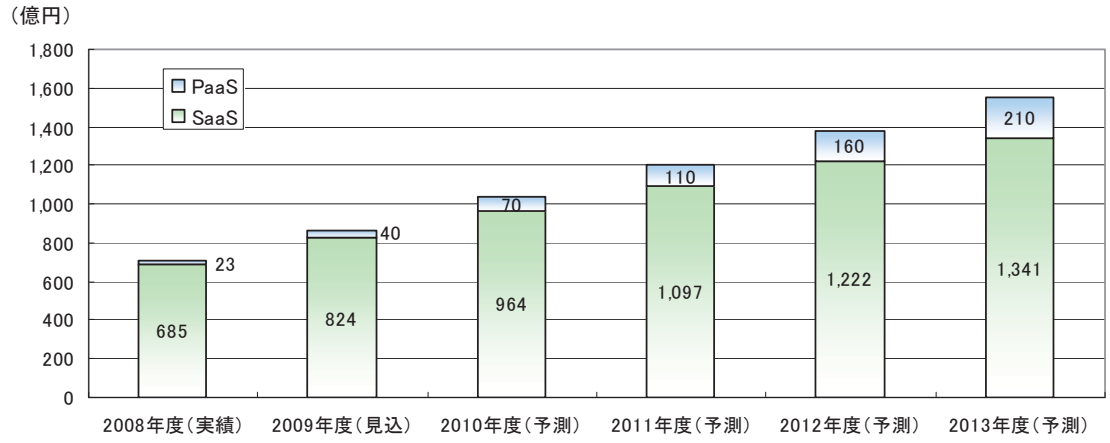
1.2.1. 国内市場規模

米国と比較すると国内企業におけるクラウド/SaaS の利用普及は後れをとったが、近年では国内でもクラウド/SaaS 関連市場規模は着実に拡大傾向を見せている。図表 1-8 に示す富士キメラ総研の調査によると、2008 年度の国内の SaaS 市場は 685 億円、2009 年度の予測は 824 億円であり、年率 120.4%で市場規模が拡大することになる。さらに、2013 年度には市場規模 1,341 億円にまで達すると見込まれている。個々のアプリケーションレベルでは、従来のパッケージ製品から SaaS への移行はユーザにとって大きな負担ではないため、国内ユーザの SaaS に対するニーズは比較的高いと言える。また、こうしたユーザニーズを見越した上で、新規に SaaS 市場に参入する事業者も増えており、今後競争の激化が予想されている。

一方で、国内の PaaS 市場は、2008 年度で 23 億円と SaaS 市場に比べて市場規模は小さいが、2009 年度の予測は 40 億円と、年率 170%を超える市場拡大を見込まれており、今後もこの拡大傾向は続くものと見られる。特に今年は国内大手ベンダ、SIer が PaaS 事業への参入を表明しており、今後サービスが本格化した際には、さらなる市場の拡大が予測される。

[4]新日鉄ソリューションズ、http://www.ns-sol.co.jp/casestudy/pdf/nssol-te-prir-doc-005-01.pdf

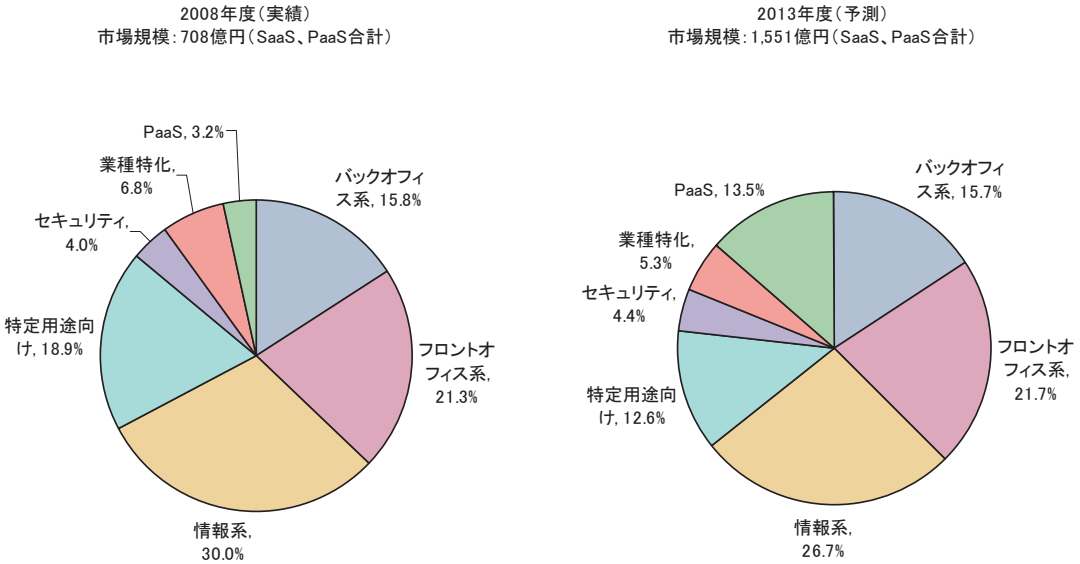
図表 1-8　SaaS/PaaS 関連サービス市場規模推移/予測（2008 年度～2013 年度）



資料：富士キメラ総研、『2009 SaaS/PaaS 関連市場の現状と将来展望』

図表 1-9 は図表 1-8 で示した SaaS 市場及び PaaS 市場の合計におけるサービスカテゴリの内訳を 2008 年度の実績と 2013 年度の予測で示したものである。2013 年には PaaS 市場は現在の 3.2%から 13.5%まで拡大することが予想されている。その他のカテゴリの割合に大きな変化はないが、市場規模自体が倍増することが予想されているため、各サービスカテゴリとも有望市場と言える。

図表 1-9　　SaaS/PaaS 関連サービス市場規模推移/予測（カテゴリ別）



資料：富士キメラ総研、『2009 SaaS/PaaS 関連市場の現状と将来展望』

1.2.2. 国内大手ベンダ、SIer の動向

Salesforce.com 等の米国大手事業者が国内でもサービス提供を拡大させる中、大手ベンダや SIer を中心とした国内事業者は、2009 年初旬から今後のクラウド/SaaS 事業戦略を相次いで打ち出し、市場への本格的な参入を急いでいる。しかしその間にも米国事業者は順調にユーザ数を拡大することでクラウド/SaaS に特有の「規模の経済」の恩恵を受けており、また施設、インフラ等にかかるコストから考えても、国内事業者が米国事業者に価格で勝負することは難しい。そこで、国内各社は事業戦略として、プラットフォームを核とした、データセンターから個々のアプリケーションまでを提供する総合的なクラウド環境の構築を掲げている。米国事業者のように、1 つのサービスモデルに特化してコスト面でのメリットを出すよりは、ワンストップですべてのサービスが利用できる環境のメリットを強調し、同時にユーザの囲い込みを図る戦略と考えられる。この場合、各社が有するプラットフォーム上に、いかに多くのアプリケーションを集めるかが重要となるため、各社とも SaaS 事業者等のパートナー作りに積極的である。但し、現在クラウド/SaaS 環境において、共通的な基準は確立されていないため、こうしたビジネスモデルでは、ユーザが特定の事業者の環境を利用すると、他の事業者への移行が難しくなるという懸念もある。

また、付加価値としてサービスの可用性、信頼性やセキュリティ等、日本企業が敏感になる部分への対応、技術力を強調し、差別化を図る傾向が見られる。

また IT 資産を外に出す事に抵抗を持つ日本企業に向けて、企業内にクラウド環境を構築するプライベート・クラウドの形態を提案し、各社が従来のシステムインテグレーション業務で得たノウハウを投入したサービスを展開している。

図表 1-10　国内大手ベンダのクラウド/SaaS の事業展開

ベンダ	クラウド/SaaS の事業展開
富士通	富士通では 2009 年 10 月より、データセンター、セキュリティ、運用管理を備えた大規模仮想化プラットフォーム「**Trusted Service Platform**」によるクラウドサービス提供を開始している。Trusted Service Platform では、以下の 4 つの分野でクラウドサービスを提供している。 **サーバファーム：** データセンター内の仮想サーバ群を利用した高信頼システム環境を提供。 **クラウドセキュリティセンター：** クラウド内の ICT 資産保護の徹底、資産評価を実施。 **インテグレーションサービス：** クラウド内システムと企業内のシステムの効率的な運用などのコンサルティング、システムインテグレーションを提供。 **マネジメントサービス：**

	リソース、ネットワーク、アプリケーションを可視化し、ユーザの ICT システムをワンストップでサポート。 富士通プレスリリース（2009.4.27）[5]
NEC	NEC では 2009 年 7 月から**「クラウド指向サービスプラットフォームソリューション」**として，顧客の基幹システムの全体最適化、「持たざる IT 化」を支援している。これは 2010 年から稼働する NEC 社内のプライベート・クラウドのノウハウを活用したものであり、具体的には、以下の 3 つのクラウドサービスを提供する。 **SaaS 型：** 定型業務をサービスとして低コストで提供する。「自治体基幹業務サービス」、「製薬業レギュレーションサービス」、「RFID 活用基盤サービス」などをメニュー化。従来、メールや e ラーニングなど業種共通のアプリケーションが多かった SaaS 領域で、NEC は各業種のコア業務・基幹業務のアプリケーションを SaaS 型で提供する。 **共同センター型：** 同一目的を持つ同業種複数の顧客が共通システム基盤上で業務アプリケーションを利用する。業種標準的なサービスを低コストで利用可能であり、自治体、金融業、メディア事業など向けに提供。主に中～大規模システム向け。 **個別対応型：** 顧客の業務プロセスを NEC のビジネスモデルコンサルタントがシンプル化・標準化した上で、複数の業務システムを NEC が提供するシステム基盤上または顧客自身のシステム基盤上からサービスとして提供。主に大規模～超大規模システム向け。 NEC プレスリリース（2009.4.23）[6]
日立製作所	日立製作所では 2009 年 7 月からクラウド関連のサービスを**「Harmonious Cloud」**として新たに体系化し、クラウド・コンピューティングの導入コンサルテーションから設計、構築、運用までトータルに提供する。具体的には、以下のソリューションを提供する。 **ビジネス PaaS：** 日立製品を中心に構成されるプラットフォームリソースの提供 **ビジネス SaaS：** 国内・海外メンバ企業 約 400 業種、約 40,000 社を有する企業間 EC 基盤。

[5] http://pr.fujitsu.com/jp/news/2009/04/27-1.html
[6] http://www.nec.co.jp/press/ja/0904/2302.html

	企業間活動に関わる業種別、役割別、利用者別に応じたアプリケーションサービスを提供する。 **プライベート・クラウド：** 企業のプライベート・クラウドの構築支援。 日立製作所ニュースリリース（2009.6.30）[7]
日本 IBM	日本 IBM では 2009 年 3 月より、顧客の IT 基盤のクラウド・コンピューティング環境移行を支援する一連のサービスを開始した。具体的には以下のサービスを提供する。 **クラウド・ビジネス・コンサルティング・サービス：** 企業のクラウド活用のあるべき姿を策定し、ロードマップを作成。 **クラウド・テクノロジー・コンサルティング・サービス：** プライベート・クラウドを環境構築のためのシステム要件定義とロードマップの作成。 **エンタープライズ・プライベート・クラウド設計・構築サービス：** IT リソースの仮想化、プロビジョニング、ネットワーク、セキュリティなど、エンタープライズ・プライベート・クラウド環境に必要な IT 基盤の設計・構築を支援。 日本 IBM プレスリリース（2009.3.12）[8] またパブリック・クラウドにおいても、2009 年 10 月より従量課金制の PaaS システムの提供を開始している。 **IBM マネージド・クラウド・コンピューティング・サービス：** 日本 IBM のデータセンターにクラウド環境を構築し、従量課金制の PaaS サービスを提供。 日本 IBM プレスリリース（2009.7.30）[9]
NTT データ	NTT データでは SaaS 事業者にサービスの実行基盤や認証・課金など共通機能を提供するプラットフォーム「**VANADIS SaaS Platform**」を構築している。プラットフォーム上では複数事業者のサービスをシングルサインオンで利用できる環境や人や組織、端末、回線など様々な要素を用いた高度な認証・アクセス制御を可能としている。 NTT データホームページ[10]

[7] http://www.hitachi.co.jp/New/cnews/month/2009/06/0630c.html
[8] http://www-06.ibm.com/jp/press/2009/03/1201.html
[9] http://www-06.ibm.com/jp/press/2009/07/3001.html
[10] http://bs.nttdata.co.jp/vanadis-saas/

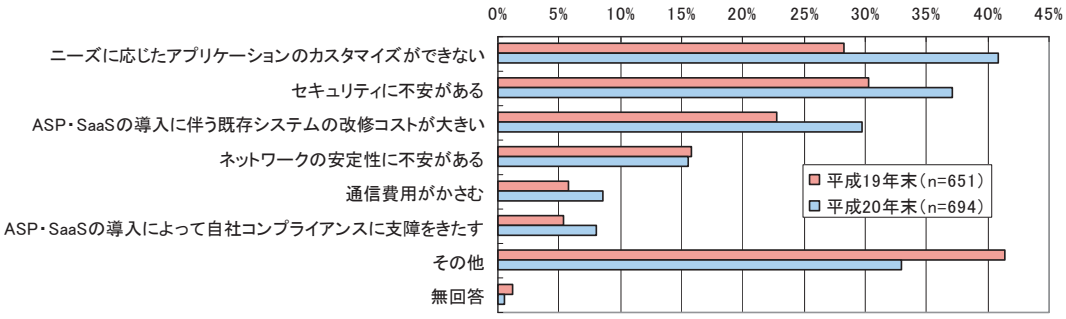
日本 HP	日本 HP では、クラウド・コンピューティング実現のために製品、サービスのポートフォリオを拡大することで「アダプティブ・インフラストラクチャ」を進化させ、社内向け、サービス提供事業者向け双方の IT 環境構築を支援している。 また、クラウド実現のための全社横断組織のタスクチームを設立しており、サーバ・ストレージ・ネットワーク・ソフトウェアなどの製品とファシリティサービスやアプリケーション開発、アウトソーシングなどのサービスを統合的に提供する体制を整えている。 日本 HP プレスリリース（2009.2.9）[11]

1.3. クラウド/SaaS とセキュリティ

1.3.1. クラウド/SaaS におけるセキュリティの課題

現在、日本企業におけるクラウド/SaaS の導入の大きな障壁となっているのがセキュリティ確保の問題である。図表 1-11 に総務省が実施した平成 20 年度通信利用動向調査企業編の結果を示す。現在 ASP・SaaS を利用していない企業における ASP・SaaS を利用しない理由として、40%近くが「セキュリティに不安がある」と回答している。

図表 1-11　ASP・SaaS を利用しない理由[12]



資料：総務省 平成 20 年度通信利用動向調査企業編

[11] http://h50146.www5.hp.com/info/newsroom/pr/fy2009/fy09-050.html
[12] 「ASP・SaaS を利用していないし、今後も利用する予定はない」と回答した企業に対する設問

クラウド/SaaS におけるセキュリティ確保は様々議論されているが、主な課題として挙げられている論点として以下の 4 点が挙げられる。これらの課題に対して、明確な対処法を示すことが、日本企業におけるクラウド/SaaS 利用拡大に繋がるものと考えられる。

(1) データの取り扱い（機密性）

事業者に対してデータの保管場所を明確にすることを求めるのは難しいが、最低限データの保管・受け渡し・返却/破棄に関する取り決めやデータの 2 次利用・海外への転送の禁止、適用される保護規制などを契約条項に盛り込めるか。

(2) コンプライアンス・監査（監査性）

クラウド/SaaS は IT アウトソーシングの一環となるため、自社データの管理責任はユーザ側にある。クラウド/SaaS 事業者に対する直接的な監査は物理的に難しい場合があるが、それに代わる有効な監査方法はあるか。

(3) 相互運用性・移植性（可用性/完全性）

社内システムや他クラウド/SaaS 事業者のサービスと連携させる際のアプリケーション間の相互運用性、データの管理・移植方法について、事業者とユーザの間で明確な合意を得られるか。

(4) 事業継続性・インシデント対応（可用性/完全性）

災害発生時や事業者が破綻した場合の対応体制やデータの保護・回収方法、他事業者への移行の流れ等について、事象者の事業継続計画を確認できるか。インシデントがあった場合の調査協力体制等も重要。

1.3.2. 政府、業界団体の動向

(1) 政府の取り組み

欧米を中心としたクラウド/SaaS の普及に伴い、2008 年頃より経済産業省及び総務省を中心にクラウド/SaaS に関わる技術、法制度等の検討が活発に行われている。主に、日本企業がクラウド/SaaS を利用する際の指針等が検討・作成されているが、それらの活動の中でもセキュリティ確保が重要な観点として取り扱われている。図表 1-12 に経済産業省及び総務省におけるクラウド/SaaS 関連の取り組みを示す。

図表 1-12　日本政府の取り組み

経済産業省	
取り組み	セキュリティに係わる検討
SaaS 向け SLA ガイドライン（2008 年）	・ 情報セキュリティ確保の観点に重点を置いた、SaaS 利用時の利用者の対策ガイドライン ・ SaaS 向け SLA におけるサービスレベル項目のモデルケースの提示
クラウド・コンピューティングと日本	・ SLA 等に関する指針、サービス選択の際の判断基準の策定 ・ クラウド・コンピューティング利活用における注意点についての

の競争力に関する研究会（2009 年）	ユーザに対する意識喚起 ・ 海外のデータセンターにデータを置く場合の機密性確保のためのガイドラインの充実
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（2009 年）	・ クラウド環境におけるセキュリティ検討会 ・ クラウド環境に適した次世代セキュアプラットフォームの検討 ・ クラウド環境活用に向けた企業内既存システムとの連携実証実験 ・ クラウド環境における効果的なセキュリティ監査技法の検討
総務省[13]	
取り組み	セキュリティに係わる検討
ASP・SaaS の安全・信頼性に係わる情報開示認定制度（2008 年）	・ 事業者やサービスを比較、評価、選択する際に必要な「安全・信頼性の情報開示基準を満たしているサービス」を認定する制度
ASP・SaaS における情報セキュリティ対策ガイドライン（2008 年）	・ 組織・運用編、技術的・物理的対策編毎のベストプラクティス及び評価項目の提示
セキュアクラウドネットワーキング技術の研究開発（2009 年）	以下のクラウド関連技術の研究開発 ・ クラウド同期型次世代 IP ネットワーク基盤技術 ・ クラウドサービス連携技術 ・ インテリジェント分散処理技術
自治体クラウド開発実証事業（2009 年）	・ 総合行政ネットワーク（LGWAN）に接続された都道府県域データセンターと ASP・SaaS 事業者のサービスを組み合わせて共同利用用途の各種業務システム等を構築し、地方公共団体が当該業務システムを低廉かつ効率的に利用できる環境「自治体クラウド」の整備に向けた実証事業
クラウド・コンピューティング時代のデータセンター活性化策に関する検討会（2009 年）	・ 国内の利用者に安心感を与えるデータセンター環境の整備
スマート・クラウド研究会（2009 年）	・ クラウド技術の標準化、相互運用性を確保するためのプラットフォーム基盤やセキュリティ基準の在り方

(2) 業界団体の取り組み

政府の取り組みとは別に、クラウド/SaaS 事業者側からの活動も始まっている。国内ではクラウド普及を目指した「クラウドサービスプロバイダ協会」や異なるクラウドサービス間の相互運用性を目指した「クラウド・ビジネス・アライアンス」が設立されている。

[13] 2009 年補正予算では「クラウドテストベッド環境（次世代クラウド・シミュレータ）の構築」に対しても予算 90 億円が予定されていたが、補正予算の見直しによって全額削減となった。

図表 1-13　クラウド/SaaS 関連業界団体

国内			
団体名称	活動の主眼	活動内容	主な参加企業
ASPIC	ASP/SaaS 普及	事業者間の情報共有 ビジネス支援（民間向け） 政策・制度立案支援 コンサルティイグ（官公庁等）	国内クラウド、SaaS、ASP 事業者多数
VMware クラウドサービスプロバイダ協議会	クラウド普及 連携強化	技術サポート・振興 共通課題に対する協業 マーケティング	伊藤忠テクノソリューションズ、NTTコミュニケーションズ、野村総研、日立情報、ソニー、ソフトバンク、日立ソフトウェアエンジニアリング、丸紅、リコーテクノシステムズ等
クラウド・ビジネス・アライアンス	相互運用性	異なるクラウドサービス（SaaS/ PaaS/ IaaS）を自由に組み合わせて利用できるクラウド間の相互接続性の実現 クラウドサービスを相互接続した際のビジネスモデルの確立 グローバルに通用する仕様	イーダブリュエムジャパン、エクシード、スマイルワークス、ネットワンシステムズ、ビープラッツ等
米国・欧州			
団体名称	活動の主眼	活動内容	主な参加企業
Cloud Security Alliance（CSA）	セキュリティ	「Guidance for Critical Areas of Focus in Cloud Computing」（2009 年 12 月第 2 版公表）の作成	eBay, ING, DuPont, HP, Sun, Dell, Intuit, Salesforce.com 等
Jericho Forum	セキュリティ	Cloud Cube Model の提唱	IBM, Dell, HP, Sun, McAfee, Salesforce.com, Zscaler, RSA Security, ING 等
Open Cloud Manifesto	オープン性	クラウド事業においてベンダが順守すべき原則の提唱	IBM, Cisco, Red Hat, SAP, VMware, ノースカロライナ州立大学, Open Cloud Consortium 等
Open Cloud Consortium（OCC）	オープン性 相互運用性	運営母体の異なるクラウド・サービスをシームレスに結び付ける標準インタフェース	イリノイ大学シカゴ校, ジョンズ・ホプキンス大学, ノースウエスタン大学, シカゴ大学, Cisco, Yahoo!等

Cloud Computing Interoperability Forum	相互運用性	クラウド・コンピューティングにおける用語の定義の検討	Cisco, intel, Sun, IBM, RSA Security 等
Open Cloud Standards Incubator	オープン性 相互運用性	クラウド・リソース管理のプロトコル、パッケージング・フォーマット、セキュリティ・メカニズムの作成	Cisco, Cirix, IBM, Microsoft, VMware 等
Storage Networking Industry Association（SNIA）/ Cloud Storage Initiative（CSI）	クラウド・ストレージ啓発/推進	クラウド管理インタフェース仕様「Cloud Data Management Interface（CDMI）」の推進、教育テキスト「Cloud Storage Tutorial」の提供	Bycast, EMC, Hitachi Data Systems, HP, LSI, NetApp, Olocity, Sun Microsystems, Symantec, Xiotech 等
EuroCloud	事業者間連携	欧州のクラウド/SaaS 事業者間の連携，情報共有	Amazon, Salesforce.com McAfee 等

米国ではさらに多くの業界団体が設立されている。特にクラウド/SaaS のセキュリティに関する検討を行う Cloud Security Alliance が公表したガイドライン「Guidance for Critical Areas of Focus in Cloud Computing」（2009 年 12 月に第 2 版公表）[14]はクラウド/SaaS 事業者及び組織のセキュリティ担当者に向けて作成された文書である。クラウドによってもたらされるビジネスの変化の中でも、組織内で「適切なガバナンス」、「リスクマネジメント」、「常識」を維持することが重要とし、クラウドセキュリティのベストプラクティスとなっている。

同文書は図表 1-14 に示す 13 のドメイン（第 1 版では 15 のドメイン）で構成されており、各ドメインについて事業者とユーザに向けた推奨事項が示されている。また、文書内では「クラウド参照モデル」という独自の参照モデルが提案されており、SaaS、PaaS、IaaS それぞれのサービスモデルに含まれる要素が定義されている。さらに各レイヤで必要となるセキュリティ技術を示すセキュリティモデル、守るべき法制度を示すコンプライアンスモデルも提案されており、3 つのモデルの関係性（図表 1-15 参照）が示されている。

図表 1-14　CSA,「Guidance for Critical Areas of Focus in Cloud Computing」の構成

第 1 章　クラウド・アーキテクチャ
Domain1 クラウド・アーキテクチャ・フレームワーク
第 2 章　クラウドにおけるガバナンス
Domain2 ガバナンス・企業リスクマネジメント

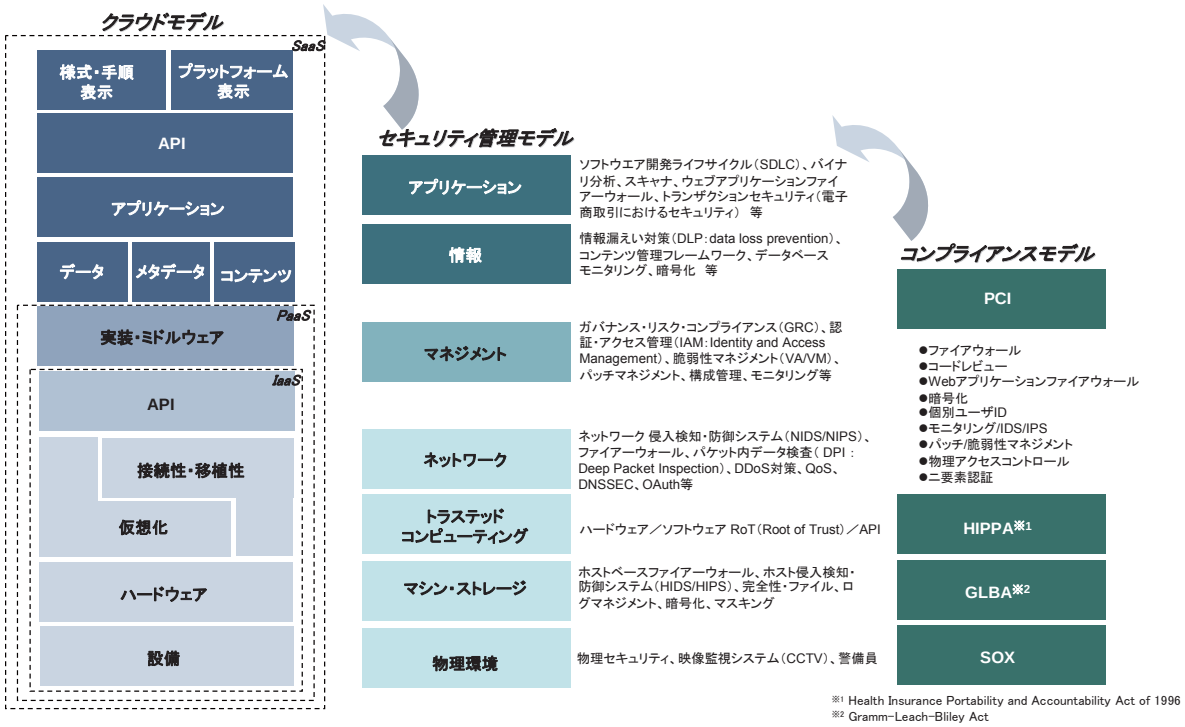
[14] CSA, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

Domain3 法務・電子開示
Domain4 コンプライアンスと監査
Domain5 情報ライフサイクルマネジメント
Domain6 移植性・相互運用性

第 3 章　クラウドにおけるオペレーション
Domain7 物理セキュリティ・事業継続・災害復旧
Domain8 データセンターオペレーション
Domain9 インシデント対応・連絡・復旧
Domain10 アプリケーションセキュリティ
Domain11 暗号化・鍵管理
Domain12 認証・アクセスマネジメント
Domain13 仮想化

資料：CSA, 「Guidance for Critical Areas of Focus in Cloud Computing」

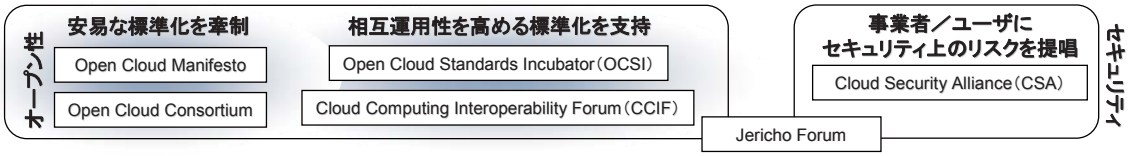
図表 1-15　クラウド（参照）モデル、セキュリティモデルとコンプライアンスモデル



資料：CSA, 「Guidance for Critical Areas of Focus in Cloud Computing」

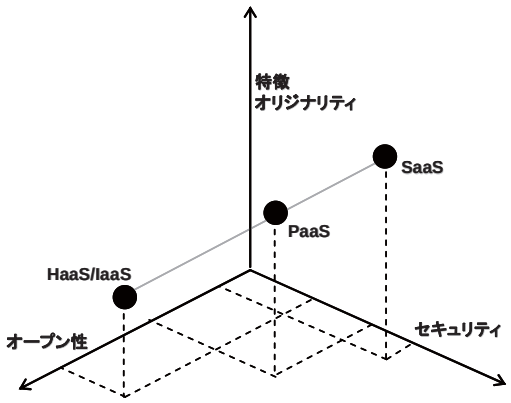
米国では上記に示すように様々な業界団体が設立される中、議論の焦点が「相互運用性」、「オープン性」、「セキュリティ」に集中している。特に「オープン性」と「セキュリティ」はトレードオフの関係にあり、クラウドの種類によってもそれぞれプライオリティが異なるため、統一的な指針を作成するのは困難である。また、クラウド/SaaS 事業者にとってみれば、自社独自の標準を維持することはユーザの囲い込みを図る 1 つの戦略である。各団体はコアメンバとなる企業がそれぞれの考え方を主張しており、各団体の動向に注目が集まっている。

図表 1-16　各業界団体の立ち位置



資料：三菱総合研究所作成

図表 1-17　オープン性とセキュリティの関係



資料：CSA, 「Guidance for Critical Areas of Focus in Cloud Computing」

1.3.3. クラウド/SaaS におけるセキュリティ関連製品・サービスの動向

ここでは、現在国内で提供されているクラウド/SaaS のセキュリティサービスの動向について紹介する。現在提供されているクラウド/SaaS のセキュリティサービスは、従来パッケージ製品として提供されていたものを SaaS に移行させたものが大半である。プレイヤとしては既存の製品・パッケージを販売していた事業者が多いが、既存の販売チャネルとの切り分けが難しい面もあり、スムーズに移行できないプレイヤもある。一方で SaaS 市場から新たに参入する事業者も増えてきており、今後の動向が注目されている。

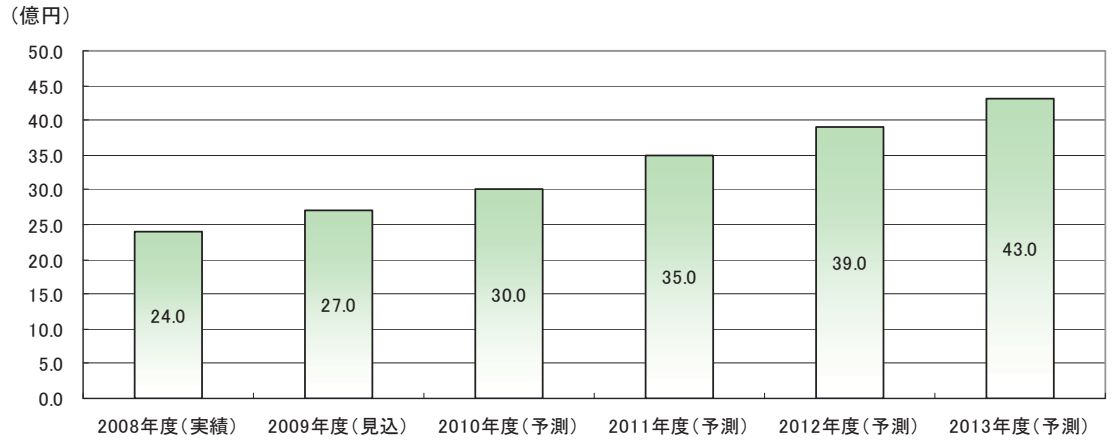
以下にクラウド/SaaS における主要なセキュリティサービスとして、ウィルス対策、ログ収集・管理及び IT 資産管理サービスの国内市場動向を紹介する。

(1) ウィルス対策

最も一般的なセキュリティツールであり、中小企業を含め法人市場における普及率は高い。価格の面だけでなく、ウィルス定義ファイルの更新がサーバによって一元化されるため、従来のパッケージ製品に比べユーザやマシンの負担が軽減されるというメリットがある。また、セキュリティ対策における基本的なサービスであるために、効率化の対象となりやすく、運用管理コスト削減を目指す中堅・中小企業のニーズを受けて市場は拡大すると予想されている。

2008 年度実績は 24 億円、2013 年度には 43 億円の市場規模[15]が予測されている。主要な参入企業はマカフィー、エフセキュア等である。

図表 1-18　ウィルス対策サービスのトータル市場



資料：富士キメラ総研、『2009 SaaS/PaaS 関連市場の現状と将来展望』

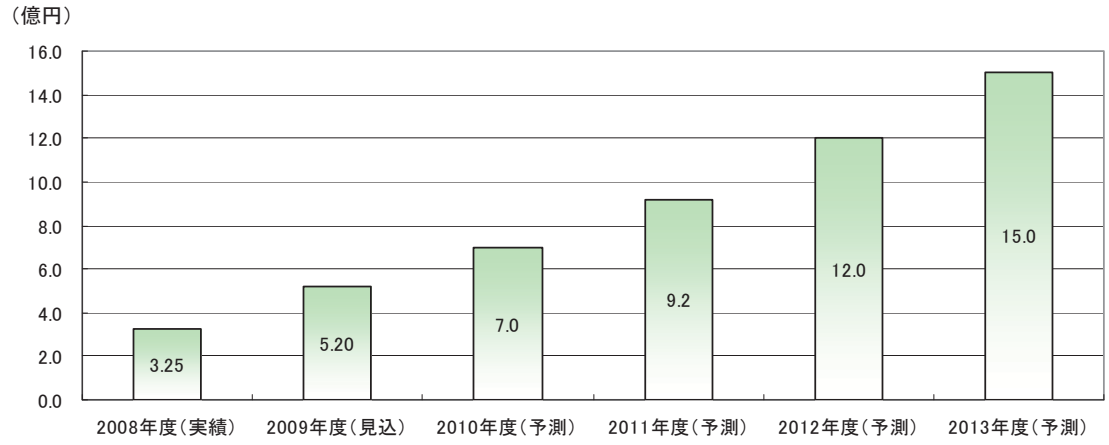
[15]Web セキュリティやメール対策ソリューションは対象外。

(2) ログ収集・管理

ログを収集・管理・分析するサービスで、主に不正アクセス防止といったセキュリティ対策やネットワーク障害対策として利用されている。最近では 2008 年から適用が開始された J-SOX 法（金融商品取引法）によって注目が集まっている。SaaS 形式でのサービス提供は 2007 年頃から開始され、一般的に初期費用が高くなるログ収集・管理ツールに比べ、安価に導入・運用可能であることからニーズが高まっている。また、今後は PCIDSS を満たすための対策としても期待されている。

サービス開始は 2007 年頃からであり、現時点では参入事業者は少ないものの、2008 年度実績で 3.25 億円、2013 年度には 15 億円の市場規模が予測されている。主要な参入事業者は NTT コミュニケーションズ、セキュアヴェイル、ソリトンシステムズ等である。

図表 1-19　ログ収集・管理サービスのトータル市場



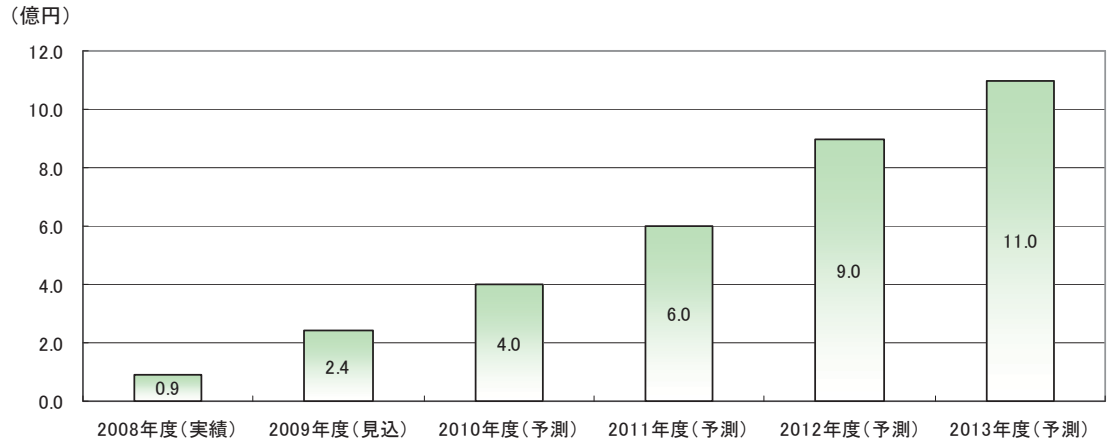
資料：富士キメラ総研、『2009 SaaS/PaaS 関連市場の現状と将来展望』

(3) IT 資産管理

クライアント PC の管理支援やセキュリティ対策を行うサービスである。主に PC 構成・管理機能、レポート作成機能、ソフトウェアライセンス管理機能、不正ソフトウェア・PC 遮断機能等を備える。(2) のログ収集・管理と同様に 2008 年に適用された J-SOX 法によってニーズが高まっているが、導入企業は大企業が中心である。パッケージ製品が、豊富な機能、カスタマイズ性を特徴としているのに対し、SaaS の場合は主要機能をベースとして、簡易なインタフェース、運用コストの削減等が優位性となっている。既にパッケージを導入している大規模ユーザの早期の移行は望めないため、未導入の企業、PC リプレイスのタイミングでの乗り換えが期待されている。

IT 資産管理の SaaS 市場はパッケージベンダからエンジン提供を受けて、参入している事業者が多く、2008 年頃から新規事業者が増加している。2008 年度実績で 0.9 億円、2013 年度には 11 億円の市場規模が予測されている。主要な参入事業者は内田洋行、サイトロック等である。

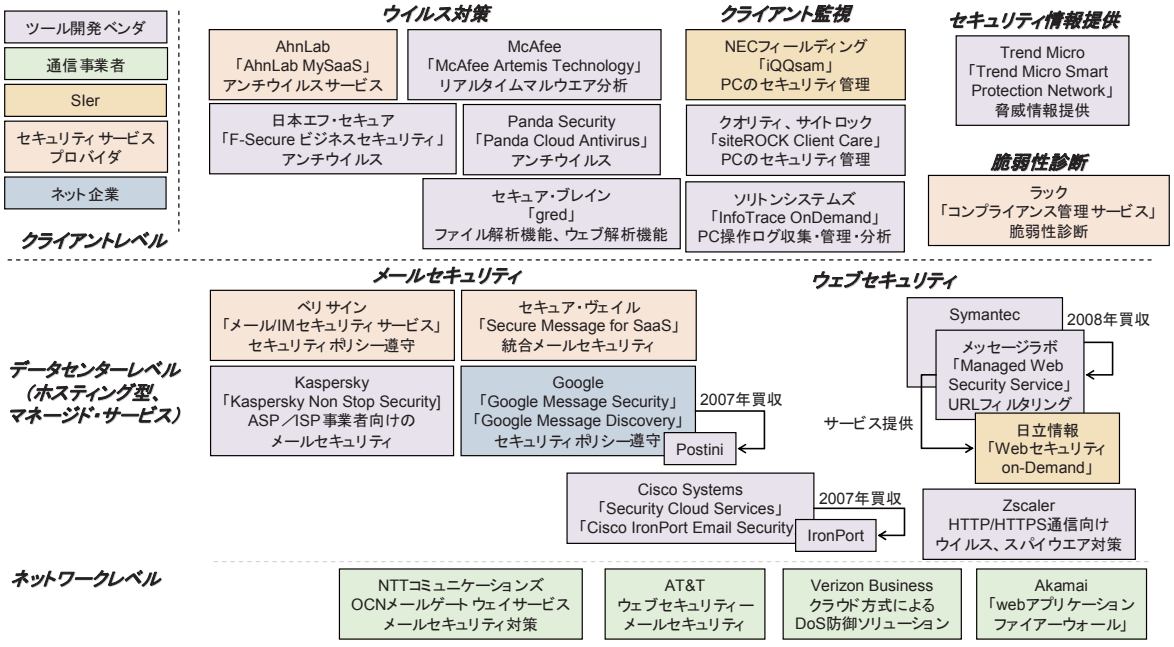
図表 1-20　IT 資産管理サービスのトータル市場



資料：富士キメラ総研、『2009 SaaS/PaaS 関連市場の現状と将来展望』

図表 1-21 に、その他国内で販売・提供されているクラウド/SaaS のセキュリティ関連製品・サービスを示す。クライアントレベルで利用される従来のセキュリティ製品を SaaS 化したものが一般的であるが、大手ではセキュリティサービスプロバイダとクラウド/SaaS 事業者が連携し、新たにデータセンターレベルでのメール・Web セキュリティを提供するホスティング型、マネージド型のサービスも提供されている。また、ネットワーク上レベルでは通信事業社を中心にファイアウォール等のサービスが提供されている。

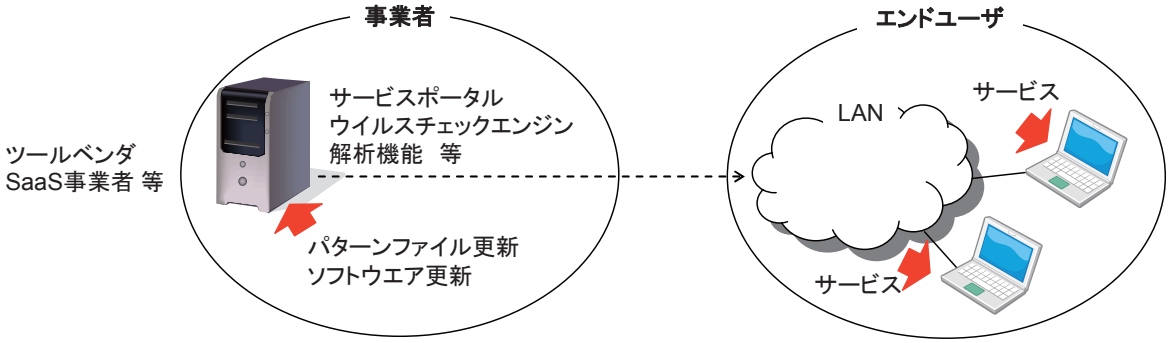
図表 1-21　クラウド/SaaS で提供されるセキュリティ関連製品・サービス



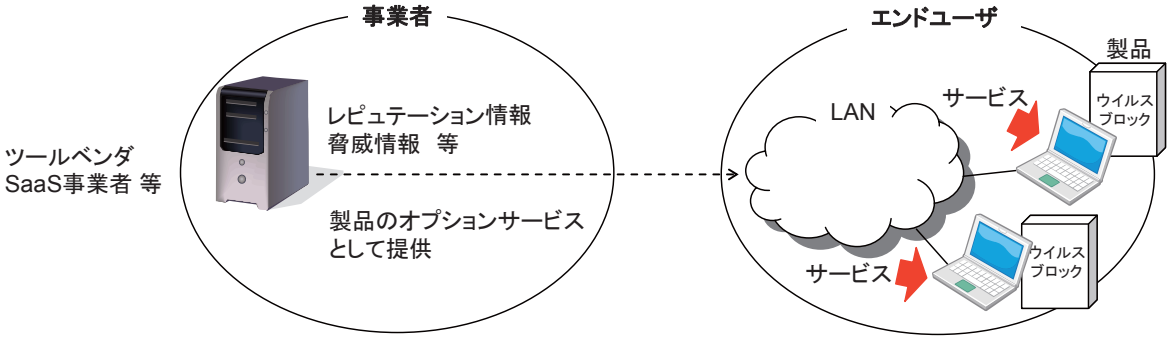
資料：各社公表資料、HP 情報を基に三菱総合研究所作成

各種サービスを提供するクラウド/SaaS 環境も様々な形態がある。ウィルス対策サービスを例にとった場合、図表 1-22 から図表 1-25 に示すように、ウィルスチェックエンジンや解析機能を完全にサーバに一元化し、ユーザが純粋なサービスとして機能を利用するものや、パッケージ製品とサーバを併用したもの、データセンターを介したサービス等の形態が挙げられる。ユーザ側では、自社のシステムに適したサービス形態を見極めることが重要となる。

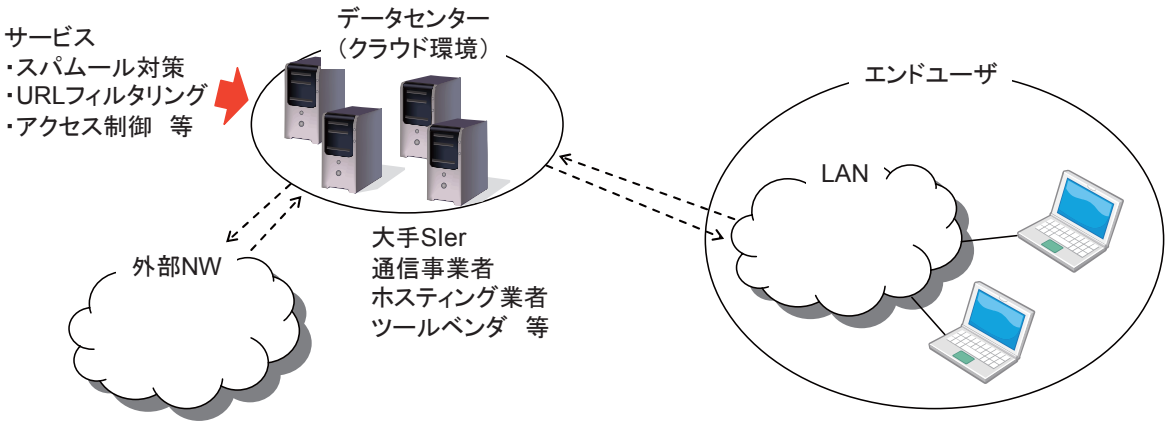
図表 1-22　クライアントレベル（SaaS 型）



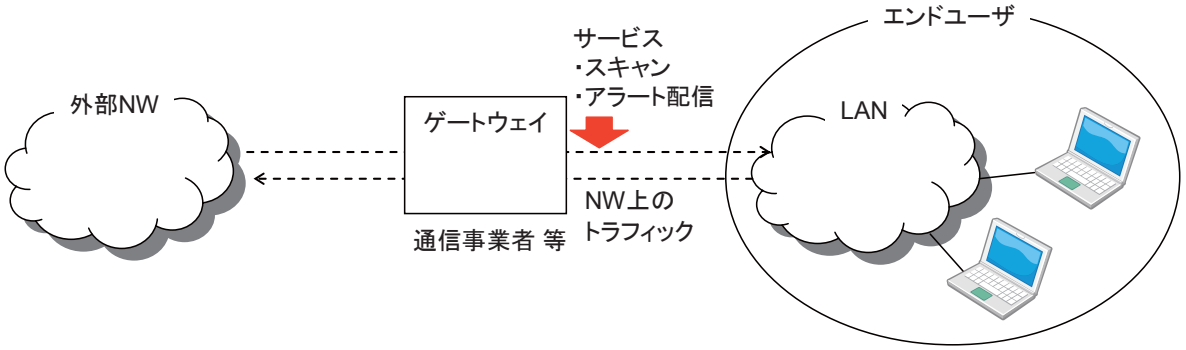
図表 1-23　クライアントレベル（SaaS/既存製品とのハイブリット型）



図表 1-24　データセンターレベル（ホスティング型、マネージド・サービス）



図表 1-25　ネットワークレベル



第２章　米国のクラウド/SaaS 主要事業者動向調査

2.1. 調査の概要

本章では、クラウド・ビジネスが先行する米国市場における、情報セキュリティ市場に影響を与えるプレイヤの動向やマーケットニーズを把握するため、米国事業者に対する調査を実施した。以下に調査の概要を示す。

(1) 調査目的

米国におけるクラウド/SaaS を視野に入れたセキュリティ関連ビジネス動向を把握する。

(2) 調査方法

米国コンサルタントの協力により、訪問または電話によるヒアリング調査を実施した。

(3) 調査対象と調査内容

本調査における調査対象及び調査内容を以下に示す。（調査対象のヒアリングメモは付録 I を参照）

【主要クラウド/SaaS 事業者】

- クラウド大手事業者：Amazon
  - サービス概要、主なユーザ層、販売・提供方法
  - 自社サービスにおけるセキュリティ確保の考え方
- クラウド・インテグレータ：IBM
  - クラウドサービスの展開状況、市場性の評価
  - クラウドサービスにおけるセキュリティ確保の考え方
- セキュリティ団体：Jericho Forum
  - セキュリティ市場全体の動向、マーケットニーズ
  - セキュリティベンチャー（クラウド/SaaS ビジネス）の動向
  - クラウド/SaaS ビジネス産業構造の現状と今後の変化
  - クラウド/SaaS がセキュリティ市場に与える影響　等

【クラウド・セキュリティ事業者】

- クラウド・セキュリティ事業者：PureWire, AlertLogic, Zscaler
  - 製品・サービスの概要、特徴、保有技術
  - 主なユーザ層、販売・提供方法
  - 社内の開発/提供体制、人材の育成・確保、提携状況
  - 現在の事業動向、今後の事業戦略・差別化戦略　等

2.2. 米国における情報セキュリティ市場の動向

米国においては、クラウド普及が先行しているが、その特徴として、特に日本市場と比較して以下が挙げられる。

- 主要なクラウド専業事業者の世界的な台頭
- 中小企業におけるクラウド利用の進展
- パブリック・クラウドの利用の増大

その背景として、米国における IT 市場の特徴が挙げられる。

- 米国ではユーザ側の情報システム部門に製品・サービス導入に関する選定能力があるが、日本においてはベンダ側が主導して選定する傾向が強い。
  - 日本ほど SIer の力が強くない。
  - 中小企業においても導入可能なサービスを提供するベンチャー等、中小事業者が活躍可能である。
- ユーザ側の業務の標準化が進んでおり、IT サービスにおける共通化が容易。

また、米国における情報セキュリティ市場の特徴として以下が挙げられる。

<u>ネットワーク脅威</u>

- ネットワークからの攻撃が多様で多い。情報窃取目的も多い。
- 政治的と想定される海外からの深刻な攻撃を時々経験する。

<u>国民の意識・カルチャー</u>

- カード支払や小切手送付支払の慣習から個人情報防衛の意識はあまり高くない一方、国家からのプライバシー干渉には敏感。
- 国防、安全保障の意識が浸透し、サイバーセキュリティ対策への官民の意識は比較的高い。
- オバマ大統領は 1 月、3 月、5 月と対策について発表し、サイバーセキュリティ重視の姿勢を示している。

<u>産業技術の特徴</u>

・インターネット・ネットワーク技術に強く、Cisco 等製品展開も巧みで世界をリード。
・ウィルス対策で Symantec と McAfee の 2 強を擁し、全般に技術競争力が強い。

<u>産業の活性</u>

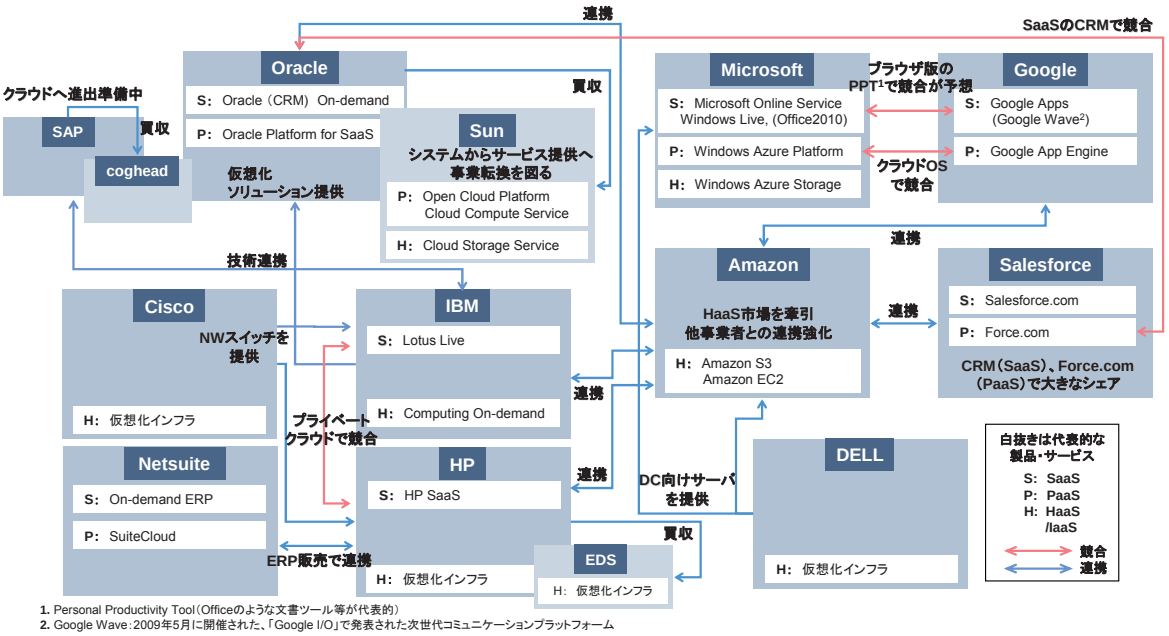
- 次の要因の相乗効果で事業規模拡大、国際競争力向上が容易
  - 国内市場大（IT 活用、Sec 対策）
  - 政府の技術開発・人材育成支援
  - ベンチャキャピタル等資金供給
- セキュリティベンダは専業が中心だが、IBM、EMC のように IT 企業が買収する例もあり、統合化が進んでいる。競争力を強める方向に働くと考えられる。

2.3. 主要クラウド/SaaS 事業者の動向調査

(1) 全体の動向

Google や Salesforce 等が先行する中、既存のハードウェアベンダもクラウド向け製品や、クラウド/SaaS 事業者へのインフラ提供に力を入れている。一方で既存ソフトウェアベンダもクラウド技術を持つ企業を買収するなどして、自社製品のクラウド転換に向けた準備を進めている。

図表 2-1　米国のクラウド業界動向



資料：週刊ダイヤモンド（2009 年 5 月 16 日号）、
各社公表資料、報道等を基に三菱総合研究所作成

(2) Amazon

提供するクラウドサービスの概要、特徴、保有技術

Amazon Web Services（以下 AWS）は Amazon.com がインターネット経由で提供する遠隔コンピューティングサービスを集約した表現である。同社では、2006 年 3 月に最初の Web サービス Simple Storage Service（S3）の提供を米国内で開始した。時間と場所に関係なく、Web 上で大容量データの保存・検索に利用可能なインタフェースとして展開した。続く 8 月には、インターネット経由でコンピュータの計算能力をオンデマンド提供するユーティリティ・コンピューティング・サービス Amazon Elastic Compute Cloud（EC2）を発表した。Amazon では、AWS における技術面での特長に関して、世界最大規模に数えられる Web サイト（Amazon.com）のインフラが基盤となっている点を強調している。Amazon.com のサイト利用者は、月間にして百万人単位にものぼり、顧客・販売者を対象とした取引もこれに比例した件数に達している。同社では、Amazon.com での経験を活かしながら、AWS の事業発展に不可欠な世界規模のインフラを開発、運営、維持するに至ったと説明している。

主なユーザ層、販売・提供方法、提携状況

Amazon によると、2007 年 6 月の時点で、AWS の利用目的で登録した開発者は 3 万 3,000 人以上にのぼる。今日、AWS を活用し、クラウド・コンピューティングにおけるサービス/ソリューション開発に取り組む独立系ソフトウェアベンダや SIer 企業のコミュニティが拡大するなど、AWS を取り巻くエコシステムが形成されている。

今後の事業戦略・差別化戦略

Amazon は、パブリック・クラウドサービス市場において主導的立場にある。Google が展開する AppEngine、Rackspace の Mosso Service とは最も強力な競争関係にあるが、Amazon は、以下に挙げる機能提供により、これらに対して優勢な地位を維持している：

- カスタマイズ機能：標準レベルに留まることなく、アプリケーションのカスタマイズ化を強みとし、新しいアプリケーションの構築能力も備えている。
- サポート力：Google の対応言語が Python のみであるのに対し、Amazon では、多岐に亘るプログラミング言語をサポートしている。
- 設定価格：Amazon では、他のキャリアが提示するものと同等の価格を維持しているが、他の項目（顧客のアカウントにおける RAM 等）を計算した場合、さらに低価格になることが多い。
- サービス内容の深度：早期参入により同分野を牽引してきた Amazon は、ストレージとコンピューティングに留まることなく、コンテンツ配信をはじめ SQS（Simple Queue Service）、SimpleDB にまでサービスの幅を拡大した。

ユーザに対するセキュリティ確保のアカウンタビリティ

AWS では、いずれのサービスにおいてもアップタイムが特定のレベルを下回る場合、（特定レベルのアップタイムを保証する）サービスクレジットとして提示される SLA を適用している。例えば、EC2 SLA では、契約が有効な 1 年間において、サービスのアップタイムを最低 99.95%の割合で保証している。上記の期間中、EC2 がこの条件を満たさなかった場合、顧客は、次月の請求金額において 10%のサービスクレジットを受ける。但し、SLA では、ダウンタイムがセキュリティやその他の問題に起因する場合は、顧客への補償を行うが、セキュリティブリーチは適用外となる。言い換えると、AWS インフラにおけるデータの完全性は、最終的には顧客側に責任がある。Steve Riley 氏（Sr. Technical Program Manager, Amazon Web Services）によると、「セキュリティブリーチは、特定の顧客が AWS で何を行っているかによって異なる場合が多いため、現時点では、攻撃に関する個別の SLA を提示していない。一方、（セキュリティブリーチ等に）影響を受けた顧客に対しては、それを最小限に抑えることができるよう、各社に対応している。勿論、Amazon EC2 のインスタンスでは、完全なルートアクセスとアドミニストレータアクセスを提供している。このため、インスタンスとアプリケーションの安全性は、主に顧客の責任となる。これによって、当社では、顧客が独自のセキュリティツールを選択できるよう、最高レベルの柔軟性を提供

している。攻撃の可能性と重大性を低減させる上では、優れたセキュリティと管理手段が最も重要になってくる」との見解を述べる他、「AWS 内部には、攻撃コミュニティにおける開発活動の監視に徹底注力したグループがある。ここでは、将来における様々な脆弱性に対応できるよう、日々、当社サービスの向上に努めている」と説明している。

セキュリティ事業者に対するニーズ

顧客におけるセキュリティへの懸念に対応するため、Amazon では、AWS フレームワークに加え、SaaS を提供する複数のソリューションプロバイダと協業してきた。中でも enStratus との提携関係は、特に重要であり、AWS/クラウドにおけるエンタープライズクラスのアプリケーションを展開・管理するためのクラウド・インフラ管理プラットフォームを提供している。この enStratus は、基幹 Web アプリケーション向けのセキュリティ、高可用性に注力したマルチクラウド・アーキテクチャを保有している。同社では、特許申請中のセキュリティ・アーキテクチャとインテリジェントな自動回復エンジン（最高 99.9999%の可用性を実現）の活用により、「クラウドに対する自信」をもたらすことを目標としている。enStratus の提供サービスにおける主要な特長には、以下のようなものがある：

- 最高レベルのセキュリティ：クラウド内部の全データを暗号化し、クラウド外部に復号化と認証の信任を維持する。
- 最高 99.9999%の可用性：ロードバランサー、アプリケーションサーバ、データベースに関しては、複数のレベルにおけるバックアップと自己修正型の回復システムを自動管理する。
- 簡単に利用可能な管理作業：ファイルディレクトリも含め、Web コンソールによって簡単に EC2 と S3 の操作・管理が可能。enStratus では、Web サービスの呼び出しに対応する他、アプリケーション管理に対するコマンドライン・ユーティリティも提供している。
- 柔軟性：アプリケーションコードへの変更を一切行わずに、Linux や WindowsOS などすべての主要なプラットフォームにおいて、いずれのアプリケーションとも動作可能。

ISV との関係について、Riley 氏は、「AWS への付加価値となるよう、多数の ISV と協力関係にあり、enStratus はその 1 社である。当社としては、これら ISV のいずれかを推薦するというのではなく、顧客自身が、パートナー企業が提供する幅広い製品（サービス）を評価した上で、自社の事業や技術面での要求に最適なものを選択するよう勧めている」と述べている。

(3) IBM

提供するクラウドサービスの概要、特徴、保有技術

世界最大規模に数えられる IT サービス企業として、IBM は、基本的なインフラ、ミドル

ウェアから利用可能な幅広いサービスに至るまで、クラウド・コンピューティングサービスにおける全般的な価値連鎖を提供している。同社では「Smart Business」として、オンデマンドによる独自のクラウド・ソリューション、インフラを展開する他、ISV（独立系ソフトウェアベンダ企業）向けに IBM のクラウド・インフラを利用して、自社のソフトウェアを SaaS へと転換させるためのツール/サービススィートも供給している。IBM のクラウドサービスは、以下「サービス」、「システム」、「コンサルティング」の 3 種に分類される。

IBM では、 競合他社との大きな差別化として、IBM Cloud Labs の存在を挙げている。大型市場及び成長市場に戦略的に配備されたこの IBM Cloud Labs は、同社のクラウド・コンピューティングに対する積極的な取り組みを示唆するものである。クラウド技術の専門家らが取り組む、完全装備の研究施設 IBM Cloud Labs（IBM では、IT 産業において最大規模であるとしている）では、セキュリティなど顧客によって異なるニーズに対応している。

主なユーザ層、販売・提供方法、提携状況

IBM は、すべての垂直産業を網羅した Fortune 500 企業向けに、エンタープライズクラスのソリューションを展開する IT サービスプロバイダとして最も知名度が高いが、同時に、中小企業や ISV 市場でも強い支持を受けている。直接販売主体の企業として知られてきたが、近年では、付加価値再販業者や技術面における提携先との協業にも力を入れている。クラウド・コンピューティング事業に対する同社の取り組みは、販売/マーケティング手法におけるトレンドと共に継続してきた。その一例として、2009 年 10 月、同社では、利用者あたり月額 3 ドルから価格設定された、電子メールサービス LotusLive iNotes を発表。中小から大企業に至るまでビジネスユーザに焦点を当てた同サービスは、安全なクラウドを利用した電子メールプラットフォームとして展開するものである。同サービスは、IBM から直接、または、同社の公式な事業提携先を通じて購入が可能である。オンデマンド型のコンピュータサービスについても、これと同様の方法で購入することができる（99 ドルのテストドライブでスタートすることも可能）。また、同ソリューションへの価値を付加する提携先を通じて、サービスを利用することもできる。提携先の Aspera（次世代伝送技術の開発企業）を例に挙げると、特許申請中の fasp プロトコルを使用した Aspera ソフトウェアでは、既存のインフラを通じて、より高速で予測可能なファイル転送を実現した。この企業では、IBM のオンデマンド型コンピューティングサービスに基づいて、自社の（オンデマンド）サービスを提供している。

提携関係の構築に対する IBM の積極的な姿勢は、チャネルパートナーに限らず、クラウド・コンピューティング業界の主要プレイヤにおいても同様である。代表的な例を挙げると、Amazon Web Services との協業により、Amazon Elastic Compute Cloud（EC2）の仮想環境において、顧客が、自社のソフトウェア製品を利用できるようになった（すべての機能とオプションが利用できる、商用版のコード）。顧客に対しては、（IBM と契約した）ソフトウェアライセンスを Amazon EC2 に持ち込む他、Amazon Machine Images を使ったソフト

ウェアの開発（ISV のみ対象）、IBM サービスを動作する製品化段階の Amazon EC2 を利用することも許可している。対応製品には DB2、Informix、Lotus、Websphere などがある。

今後の事業戦略・差別化戦略

IBM の戦略では、プライベート/パブリック・クラウドの両方を網羅している。IBM では、コンピューティングやストレージなどパブリック・クラウドのリソースを提供すると同時に、プライベート・クラウドの構築に向けた総合的なソリューション（Cloudburst）も展開。その一方で、IBM では、プライベートとパブリック・クラウドにおける中立状態の維持にも努めている。Kristin Lovejoy 氏（Director, IBM Corporate Security Strategy IBM CloudBurst Project Office）は、「顧客側では、プライベート・クラウドに対し、自社で一貫した制御ができる上、ファイアウォールの背後に置かれていることから、性能と安全性の両面で優れていると捉える向きがあるが、実際には、セキュリティに特化して精巧にカスタマイズ化された SLA では、これと同等の安全性を確保している。また、パブリック・クラウドに関して言えば、顧客側でスケールメリット基づいた価格交渉ができるため、さらに効率性が高く、安価なものになる可能性もある」と述べている。

ユーザに対するセキュリティ確保のアカウンタビリティ

IBM では、自社のクラウドサービスにおける各局面を網羅した SLA によって、顧客へのアカウンタビリティを保持している。これについて、Lovejoy 氏は「SLA は、クラウドのベンダ企業が、顧客毎に異なるビジネスニーズを理解し、それを着実に実行するような内容で構成されるべき」だと指摘し、同社では、以下の項目に対応するよう提案している：

- 可用性及びアップタイム
- サードパーティの介在など、インフラ管理を実行する組織の把握
- データセキュリティ（特に、サードパーティやその提携先におけるデータの取り扱い方法）
- ベンダ企業における責任（誰が何に対して責任を負うのかの明確化）
- ベンダ企業やサードパーティが倒産した場合の規定
- データの移行とその取り扱い方法
- 顧客のデータが、地域や国の境界を越えて流出した場合、その境界領域とアクセスに関する制約（国や州によっては、特定地域からデータが流出することを禁止）

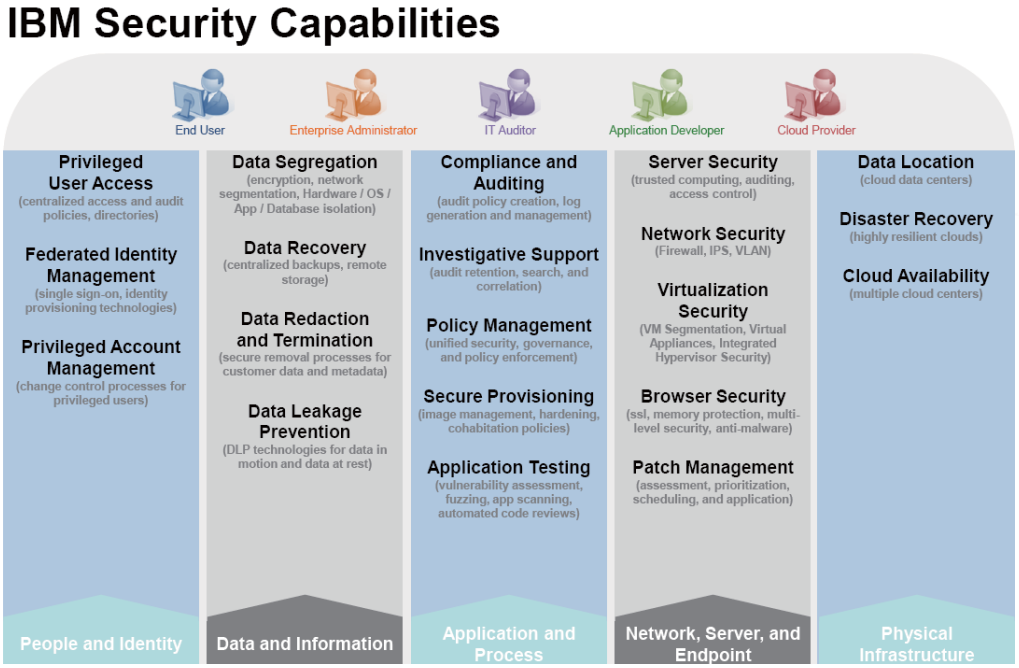
Lovejoy 氏は、SLA について、アカウンタビリティの確立において重要な要素であるとし、「契約によって異なるが、（IBM に限らず）通常、合意した SLA の中では、サードパーティのプロバイダが、セキュリティブリーチの発生時に、誰が責任を負うかを具体的に定義している。このため、顧客がこれ（責任の対象）を懸念するのであれば、SLA の中に必ずその内容を盛り込んでおく必要がある。また、これは、クラウド・コンピューティングに限って適用されるものではない。顧客がサードパーティにデータを提示する際は、いずれ

の場合においても、SLA でこの問題に対処しなければならない」と説明している。

セキュリティ事業者に対するニーズ

IBM では、顧客が懸念するクラウド・コンピューティングでのセキュリティ関連問題を的確に把握した上で、先に述べた IBM Security Framework の他、自社のセキュリティ製品（外部のパートナーに殆ど依存する必要が無い）を利用して、これらに対応している。以下の図表では、同社が提供する多様なセキュリティ機能を概説している：

図表 2-2　IBM が提供するセキュリティ機能



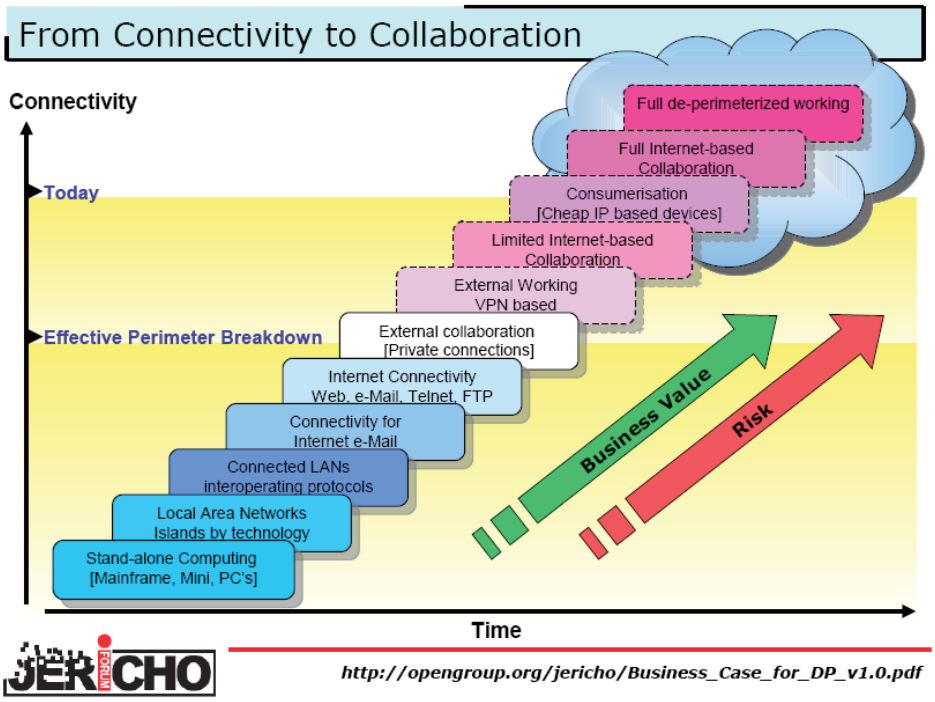
資料：IBM

（4） Jericho Forum

クラウド普及に向けた取り組みの概要

Jericho Forum は、グローバル企業の CISO ら（最高情報セキュリティ責任者）が集結し、ネットワーク境界の侵害に対する企業システムの防御コンセプト（以下 de-perimeterization：多様な通信活動を要因にファイアウォールの弱化が発生している状態。以下の図表を参照）について、対処すべき問題を議論する場として、2003 年にスタートした。インターネット経由での安全な事業展開を目指す一方、企業のネットワーク境界における継続的な侵害問題に対応するため、これらの CISO らが率先する形で Jericho Forum を設立した。「Senior IT Security Officers Working Together to Help Businesses Succeed」をスローガンに掲げる同フォーラムには、今日、欧州をはじめ北米、アジア太平洋地域における顧客企業、サプライヤ、政府機関などが会員として参加している。

図表 2-3　De-perimeterization の考え方



資料：Jericho Forum

同フォーラムでは、今日のビジネス環境における成功は、インターネットを経由した安全なデータ伝送の実現による協業と事業展開能力に依存している、との基本概念を持っている。2004年、提携先をはじめ顧客、サプライヤ、外部委託者を含む企業各社が世界規模で安全に協業できるよう、安全性を追究したアーキテクチャ、技術ソリューション、実装におけるアプローチの開発を立案・主導すると同時に、これらソリューションの基盤となるオープン標準の開拓を促進するようになった。その後、クラウドを利用したアプリケーションへの高い関心を認識し、2009 年よりクラウド・コンピューティングにも取り組むようになった。

現在、Jericho Forum におけるミッションは、以下のような活動を通じて、会員における全体的な将来展望の達成を促進することにある：

- リーダーシップを通じた問題空間の特定。
- 会員全体における将来展望についての話し合い。
- 様々な制約に取り組み、技術革新に向けた環境の構築。
- 市場の確立。
- 将来におけるアーキテクチャ、サービス、製品、標準に対する影響力の促進。

クラウドサービスにおけるセキュリティ確保の在り方

Jericho Forum では、1)．de-perimeterized 環境での IT アーキテクチャを確保する手段の評価用として、設計原則を定義した一式の戒律 The Jericho Forum Commandments、2)．同フォーラムの戒律を満たす安全なアーキテクチャの設計に関して Collaboration Oriented

Architectures（COA）Framework を発表した。

将来の de-perimeterized に関する計画を考案する際、順守すべき領域と原則が定義されている。「優れたセキュリティ」を基盤とする一方、この戒律では、特に、de-perimeterized に対する構想の実現に必要なセキュリティ領域に対処している。 評価や測定可能な概念、ソリューション、標準、システムに応じたベンチマークとしての役割を担っている。以下では、これを構成する 11 の戒律に関する概要を示した：

- 危険にさらされている資産に特定・適切な保護の範囲とレベルの適用を義務付ける。
- セキュリティの構造は、広範囲で、拡張性を備え、シンプルかつ簡単に管理できるものでなければならない。
- IT インフラのセキュリティ環境を予測することは危険である。
- 機器及びアプリケーションに関しては、オープンで安全なプロトコルを使用した通信が義務付けられる。
- すべての機器においては、不信用と判断されるネットワークに対し、セキュリティポリシーの維持能力を備えることが条件。
- 関係者、プロセス、技術のいずれにおいても、実行するトランザクションに関しては、すべて認証を受けた透過的な信用レベルに達することが義務付けられる。
- 相互における信頼関係を保証するレベルは、特定するよう義務付けられる。
- 認証、許可、説明責任は、制御を実行する領域外部で相互運用/交換されるものとする。
- データアクセスは、データ自体のセキュリティ属性によって制御されるものとする。
- データに関するプライバシー（及び、価値が十分に高いすべての資産におけるセキュリティ）では、責務と特権の分離を必要とする。
- 初期設定において、データは保存段階及び伝送段階のいずれにおいても適切に保護されることが義務付けられる。

The Collaboration Oriented Architectures（COA）Framework

Collaboration Oriented Architectures Framework では、以下の点に焦点を当てた一式の設計原則を提示している：

- 増大するコラボレーションに起因したセキュリティ問題に対する防御。
- Web 2.0 の他、社外でも使用される技術（Externalization Technologies）がもたらすビジネス機会の活用。

同フレームワークは、各組織に対し、個別のニーズに合致する方法で、安全なビジネスコラボレーションを立案する手法の紹介に注力したものである。COA の展開は、効果的かつ安全なコラボレーションを実現するよう、既存の標準と慣例を基盤としている。Jericho Forum における次の目標は、クラウドにおける安全なコラボレーションに対応した、最優良な原則一式を開発することである。

前述の通り、この COA は、ビジネスを目的とした安全なコラボレーション向けのアーキテクチャを考案する際、その最良策を提案することに焦点を絞ったフレームワークである。制定された COA Framework（COA）v2.0 は、以下の要素で構成されている。

Jericho Forum では、クラウドサービスに対する大企業のニーズを分析するため、Cloud Cube Model と層状モデルを開発している。Stephen Whitlock 氏（Board of Management of the Jericho Forum の会員）によると、「クラウド・コンピューティングに対しては、インターネットを経由したあらゆるサービスを網羅するようなイメージがあるため、これ（クラウド・コンピューティング）に関する多くのディスカッションは、複雑になっている。こうした状況に対応するため、Jericho Forum では相互運用性に関する問題、データやサービスの位置、サービスの構成方法などクラウド・コンピューティング内部の様々な側面や特性を検証する Cloud Cube Model を開発した。これらは、クラウドサービスにおける階層的なレイヤ（ファイルサービスを下層とし、順次、開発サービス、アプリケーションがその上層を成す）を検証する層状モデルと連結されている。

これらの側面や特性を紙上で組み合わせると、3 面や 4 面以上になるため、複雑にはなるが、特定のクラウドサービスが実行可能であるか、を判断する上で役立つものである。例えば、クラウドサービスの構築能力を持たないが、社内で実現したいという企業に関しては、クラウドサービスの提供業者に開発作業を委託することになる（プライベート・クラウドを利用するケース）。一方、クラウドサービスの迅速性を有効活用したいが、社内のインフラは持ちたくないという企業においては、パブリック・クラウドを利用することになる。

先に述べた層状モデルにおいては、より簡単に外部委託できるレイヤもある。例えば、ストレージに関しては、外部のセキュリティに依存することなく、暗号化のみで対応できる。一方、アプリケーション開発の場合は、クラウド内部でコードを動作させる必要があるため、当然のことながら、暗号化を行うことはできない。企業においては、自社ビジネスの要素において、暗号化やエクスポート保護が必要な部分、その他の領域も検証した上で、クラウド・コンピューティングに適合するものを特定すべきである。従って、Personally Identifiable Information（PII：個人を識別できる情報）などは、クラウドの高層にあたるアプリケーションレベルで移動させることが困難な領域かもしれない」と説明している。

(5) まとめ

米国のクラウド/SaaS 市場では、大手クラウド/SaaS 事業者が先に台頭したことにも伴い、パブリック・クラウド市場が日本より早期に形成され、中小企業においても利用が促進されている状況にある。そのような中、クラウド/SaaS 事業者に対して日本のユーザが抱える課題の 1 つであるサービスのセキュリティレベルについては、いずれのクラウド/SaaS 事業者においても大規模なセキュリティ投資を行っており、自社保有技術で対応する場合と、提携事業者により向上させるケースがある。しかしながら、その内容や費用などの詳細は

明らかにされず、外部事業者に委託するニーズについても現時点ではわからない点は多い。また、ユーザに対するセキュリティ確保のアカウンタビリティは、個別ユーザ毎に定める場合と、SLA で定める場合とがあり、これも事業者の意向によって異なる。

SIer におけるビジネスという点では、日本と米国ではそもそもユーザ企業と SIer の関係が異なる背景もあり、単純な比較は難しい。しかしながら、米国の大手 SIer は概ねハードウェアを保有している場合が多く、日本と同様にプライベート・クラウドを含めた、既存システムのクラウド・インテグレーションを視野に入れたビジネス展開を開始している状況である。

2.4. クラウド・セキュリティ事業者の動向

米国では、セキュリティ事業者がクラウドビジネスを展開し始める例が見られる。本節では、クラウド・セキュリティビジネスを展開する米国事業者の例を紹介する。

(1) PureWire

会社概要

2007 年設立、従業員数 50 名、拠点はアトランタ

事業概要

特に中規模からエンタープライズクラスの企業に焦点を当てたインターネット利用におけるセキュリティ、性能、制御能力の強化を求めるソリューションを提供。SaaS 型 Secure Web Gateway として展開される同社の Web Security Service は、企業ネットワークとインターネットの間に置かれ、ビジネスに必須な Web 利用においてユーザを保護する。アウトバウンドの Web トラフィックに関しては、安全性と規制遵守を審査する一方で、不正なプログラムや不信なユーザに関するレスポンストラフィックの分析を実行する。管理者側では、直感的な Web インタフェースを使用し、同社サービスの監視、管理が可能になる。

主なユーザ層

複数の Fortune 1000 企業も含め、零細企業から大企業に至るまで幅広い顧客を有する。

提携状況

主要な提携先である Reflexion 社（IT ソリューションを提供）では、同社との OEM 契約を通じて、独自の Web セキュリティサービスを展開。

保有技術

URL Filtering、Data Leak Prevention、Application Control（ブラウザを利用しない Web アプリケーションを含む多様な Web アプリケーションへのアクセス管理）、Bandwidth Control、

Compliance Enforcement（ユーザに許可するタスク等を統括した、カスタマイズ対応のルール対応管理）、The Dynamic Response Classifier Engine（HTTP ヘッダ、コンテンツフィルタリング、リンク解析によるレスポンストラフィック分析）、The Threat Analyzer Engine（特定のアプリケーションにおける動作を正確に判断するよう、ブラウザのエミュレートと同時に、複数のセキュリティチェックを実行）、Object-based Malware Detection、Signature-based Anti-Virus 等

今後の事業戦略

経営手腕を備えると同時に、同分野に精通した人物らが運営。「クラウドにおける脅威の効果的な回避技術」として同社が宣伝する通り、現在までその領域では成功を収めている。今後、ハードウェアを利用した従来のソリューションに対して、大きな競争力になるものと予測される。

(2) AlertLogic

会社概要

2002 年設立、従業員数 100 名、拠点はヒューストン

事業概要

簡単に導入・利用できるオンデマンドサービスとして、規制遵守とセキュリティに対応したソリューションを提供。Alert Logic Log Manager は、ログデータにおける収集、定期的な再審査、安全な保存が条件とされる PCI、SOX、HIPAA、GLBA 等の規制遵守に適用される。解析・検証用として同一の情報を生成し、全般的なセキュリティと可用性の向上を目指している。一方、Alert Logic Threat Manager では、ローミング対応のラップトップ機器や VPN 接続、無線アクセスポイント、提携先の Web ポータル、本来、信用できるはずのソースに起因したウィルスやワーム等から内部ネットワークを常時保護する。これと同時に、外部ネットワークとの境界やエンドポイントの防御を簡単に迂回する脅威に対しては、ネットワーク防御の基幹レイヤを構築。2009 年 2 月、2 年連続で SAS 70 Type II Audit を完了したと発表。PCI SSC（PCI Security Standards Council）が認定したスキャニングベンダ企業（Approved Scanning Vendor）でもある。

主なユーザ層

エネルギー、技術、ヘルスケア、リテールなど非常に幅広い産業で顧客を拡大。規制準拠に対する同社の取り組みが顧客拡大の大きな要因であり、リテール産業においては、PCI DSS への準拠が導入実績の増加に繋がった。

提携状況

Ingram Micro 社の北米における 4 万社以上のソリューションプロバイダ、マネージドサー

ビスプロバイダに提供。複数の Web ホスティング及びマネージドサービスの提供業者と提携関係にある。

保有技術

SaaS ソリューションは、ログ、脅威、脆弱性データを収集し、処理するようデータセンターへと転送するオンプレミス（自社運用型）のネットワークアプライアンスで構成。同社のデータセンター内でホスティングされ、世界に点在する全顧客のアプライアンスからのデータを解析し、安全に保管する。この他、同コンポーネントでは、顧客の Web ポータルを通じて、リアルタイム及び過去の動向データやレポーティングも提示する。

Log Manager は、ネットワークに接続された PC（ローカル）でログデータの収集、アグレゲーション、圧縮を実行した後、企業のデータセンターにおいて、それらの処理、解析、報告、検証、安全な保存を一貫して行うオンデマンド型ログ管理としては、業界初の技術である。

Threat Manager では、侵入脅威への保護と脆弱性の管理技術を単一のソリューションに統合。Alert Logic ネットワーク機器が発信するすべての警告は、同社のデータセンター内部でホスティングされた集中管理型の専用システムへと直接、伝送される。その後、この専用システムでは、IDS 警告データを、世界に広がる Alert Logic の全ユーザから収集した、脆弱性情報とリアルタイムの脅威に関する動向データに相関させ、セキュリティ問題を的確に特定。このため、誤検出の可能性が低減するとされている。

今後の事業戦略

他の SaaS と同様、同社でも迅速な導入とゼロ保守を特長に、前払いの資本コストを必要としない点も強みとしている。同社は、中小規模の企業に注力している。ホスティングパートナー企業とは強い繋がりを確立し、ログ管理の分野でも認知度が高い。

(3) Zscaler

会社概要

2007 年設立、従業員数 90 名、拠点はカリフォルニア

事業概要

クラウド・コンピューティングにおける様々な安全性問題に対応した「サービスとしてのセキュリティ技術」を提供。オンプレミス（自社運用型）のセキュリティソフトウェア及びアプライアンスの代替技術として展開している。SaaS 型のセキュリティサービス Global Security Network では、企業の Web トラフィックを同社のデータセンターの一拠点にリディレクトし、各社毎に異なるポリシーに従って、トラフィックの許可や遮断を実行。このため、多点（マルチ）のセキュリティ製品が不要となる。

主なユーザ層

既存顧客は、大小規模の企業を主体としている。大～中規模企業では、従来の多点セキュリティ製品を排除するため、また小規模企業については、IT 管理者を雇用することなく、既存ソリューションの管理・更新に要する費用を削減する技術として評価が高い。

提携状況

Microsoft 社との提携関係を通じて、Microsoft Active Protections Program（MAPP：セキュリティベンダを対象に、月例で事前に脆弱性情報を開示するプログラム）を利用、数あるパートナーシップの中でも重要な提携関係とされている。

保有技術

エンタープライズでのセキュリティに関しては、通常、マルウェアや侵入者の走査ツール（抗ウィルス、アンチスパイウェア等）を利用し、安全な境界を確保するよう、様々なアプリケーションと機器（ファイアウォール、ゲートウェイ、ネットワークアクセス制御、VPN 等）が介在している。同社の技術では、自社のセキュリティインフラを経由したトラフィック伝送により、これらの一部を削除することができる。

分散型のマルチテナントアーキテクチャを採用した同社製品は、①Zscaler の様々なアプリケーションがトラフィックのフィルタリングを実行する際、遅延を最小限に抑える Single-Scan Multi-Action (SSMA) Gateway、②ウェブログの規模を最大 50 倍まで圧縮可能な NanoLog が主要な技術となっている。これらの技術が一体となり、受信・送信の Web トラフィックに対する IT ポリシーを適用する際に、作業時間の短縮と高拡張性が実現される。

今後の事業戦略

2009 年 8 月、エンタープライズを対象に Infonetics 社（国際市場の調査会社）が実施したアンケート調査の結果、同社は、SaaS 型セキュリティサービスプロバイダにおける上位 4 ブランドの 1 つに選ばれたと発表。同調査の結果では、費用性能比、サービス及びサポート、企業としての財政的な安定感など様々な基準において、同社は、Cisco 社、TrendMicro 社、Symantec 社など複数の大手セキュリティベンダを抑え、トップレベルに位置している。

第３章　情報セキュリティ製品・サービス 利用状況・意向調査

3.1. 調査の概要

本章では、クラウド/ SaaS 利用におけるセキュリティに関する課題やセキュリティ確保のポイント明確化やクラウド/ SaaS 時代における情報セキュリティ市場性を把握するため、日本のユーザ企業におけるクラウド/SaaS の利用動向、さらにクラウド/SaaS を利用している企業における導入方法や、利用における管理方法等を調査した。日本企業全体における利用動向を把握し、同時に実際の利用者の状況を深く探るため、本調査は以下に示すように 2 段階に分けて実施された。

(1) 調査方法

調査は 2 段階のウェブアンケート調査で実施し、対象者は goo リサーチビジネスモニタ[16]から以下の条件で抽出した。第 1 次調査では、社内担当者に対して社内のクラウド/SaaS 利用の有無、利用意向を聞き、第 2 次調査では第 1 次調査においてクラウド/SaaS を利用している、或いは利用を検討していると回答したモニタを対象に、詳細な利用状況を聞いた。（本調査の調査票は付録 III を参照）

(2) 調査対象

goo リサーチビジネスモニタから以下の対象者を抽出した。

■第 1 次調査：

- 社内向けシステム・情報システム企画運用管理担当者　及び、
- 自社内 IT システム導入を決定する、または導入を検討し推薦する立場にいるソリューション・システム企画、設計、開発、運用管理者

■第 2 次調査

- 第 1 次調査の回答者のうち、問 1 の回答が「クラウド/SaaS を利用している」または、現在利用していないが、今後利用を検討している」と回答した回答者
- かつ、従業員数 50 人以上の企業

(1) 調査期間

■第 1 次調査（「あなたの勤務先の情報システムに関する調査」として実施）

- 2009 年 11 月 5 日～11 月 6 日

■第 2 次調査（「クラウド/ SaaS 利用に関する調査」として実施）

- 2009 年 11 月 10 日～11 月 13 日

(2) 回収数

■第 1 次調査：2,403 件

■第 2 次調査：305 件

そのうち、第 1 次調査における問 1 の回答が、

[16] goo リサーチビジネスモニタ：https://research.goo.ne.jp/monitor/about_m.html

・ 「クラウド/SaaS を利用している」: 152 件
・ 「現在利用していないが、今後利用を検討している」: 153 件

3.2. 日本のユーザ企業におけるクラウド/ SaaS 利用実態[17]

3.2.1. 調査結果

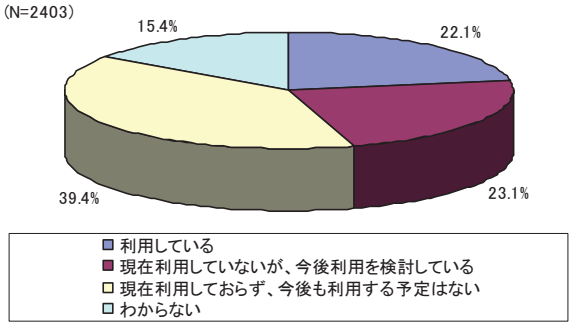
(1) ネットワーク上のサービス（クラウド/SaaS）の利用動向（第 1 次調査）

第 1 次調査では 2,403 名の回答者に対して、クラウド/SaaS の利用動向について調査を行った。ここでは、回答者がクラウド/SaaS をよりわかりやすくイメージできるように「クラウド/SaaS」という表現の代わりに、「ネットワーク上のサービス」という表現を用い、これを「ユーザがネットワークを通じてリソースを意識せずに利用できるサービス（クラウド・コンピューティング、SaaS: Software as a Service、ASP: Application Service Provider 等）」と定義した。

第 1 次調査の回答者のうち、現在クラウドを「利用している」と回答した割合は 22.1%、また「現在利用していないが、今後利用を検討している」と回答した割合は 23.1%となり、半数近くが、クラウド/SaaS 利用に対して積極的な姿勢を見せている。一方で「現在利用しておらず、今後も利用する予定はない」（39.4%）と回答した回答者にその理由を聞いたところ、「必要性がない」との回答が 68.8%を占めた。

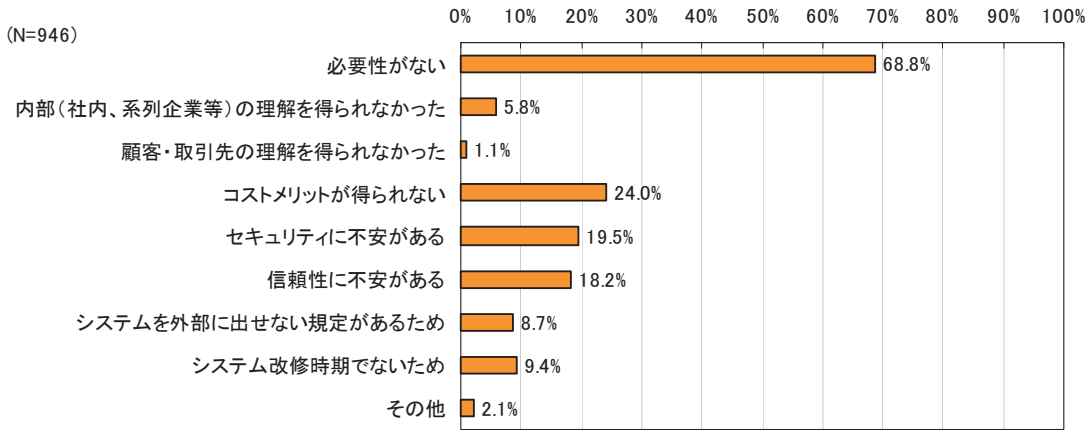
日本企業における現在のクラウド/SaaS の利用は、比較的導入に積極的な企業と、そもそもの必要性を感じないため、検討も行わない企業とに二極化している状況がある。

図表 3-1　クラウド/SaaS の利用動向



[17] 本調査の単純集計結果は付録 III を参照。

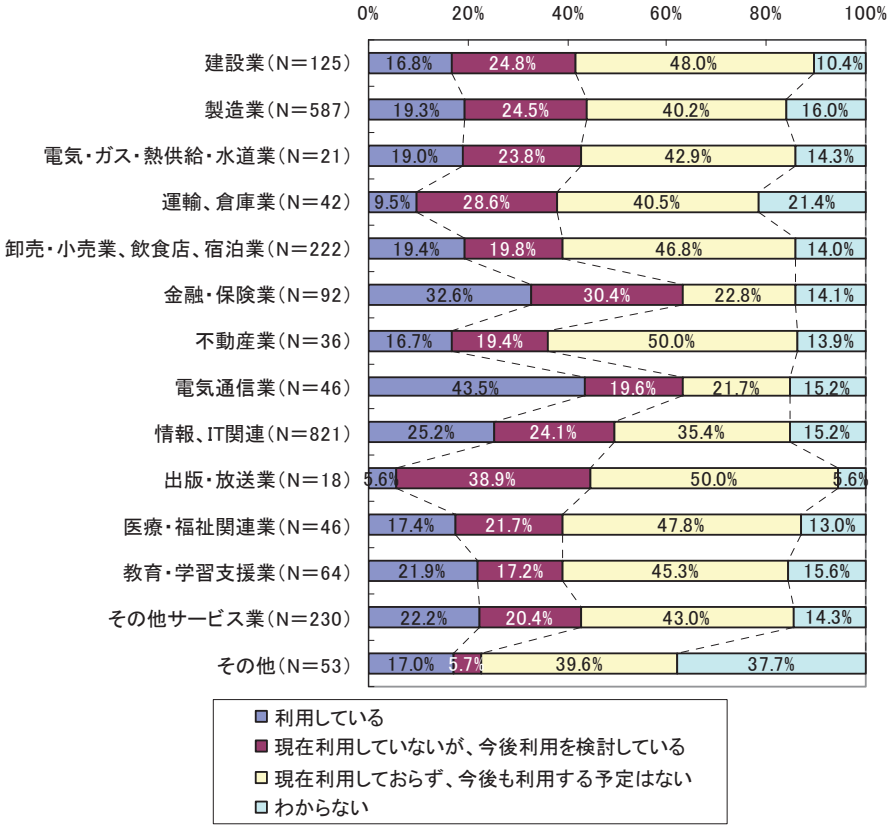
図表 3-2　クラウド/SaaS を利用しない理由



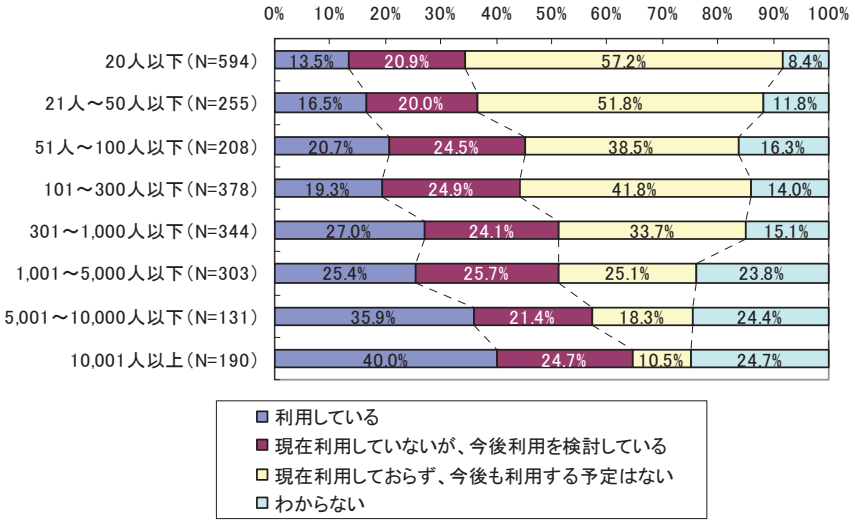
(2)　ネットワーク上のサービスの利用者プロファイル（第 1 次調査）

ネットワーク上のサービスの利用率は、電気通信業、金融・保険業、情報、IT 関連企業の順に高く、IT を利用する機会の多い企業での利用が目立つ。また、従業員数の多い大企業ほど利用率が高い傾向にある。参考として、図表 3-5 に回答者の企業の従業員数とネットワーク上のサービス利用状況別に従業員数の分布を比較している。

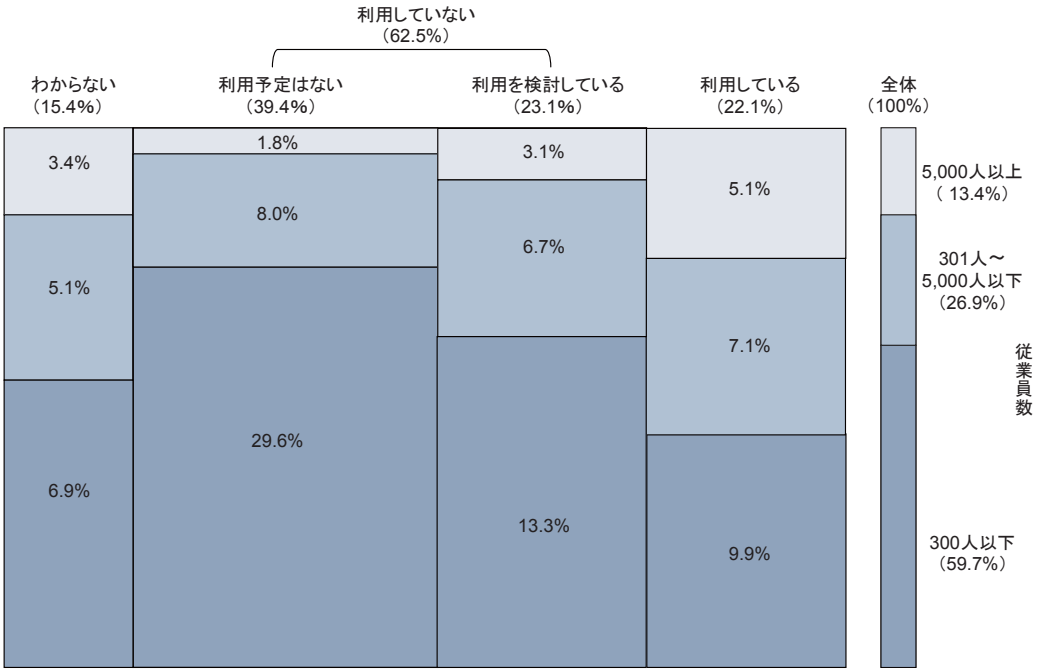
図表 3-3　業種別ネットワーク上のサービス利用の状況



図表 3-4　従業員数別のネットワーク上のサービス利用の状況



図表 3-5　第 1 次調査回答者（N=2,403）



(3)　業種別クラウド/SaaS の各サービスの利用状況（第 2 次調査）

第 2 次調査では、第 1 次調査においてネットワーク上のサービスを「利用している」または、「現在利用していないが、今後利用を検討している」と回答した 305 名に対してサービス別の利用状況・利用意向を調査し、さらに「利用している」と回答した 152 名に対して、詳細な利用状況を調査した。

第 2 次調査においてはクラウド/SaaS を以下のように定義した。

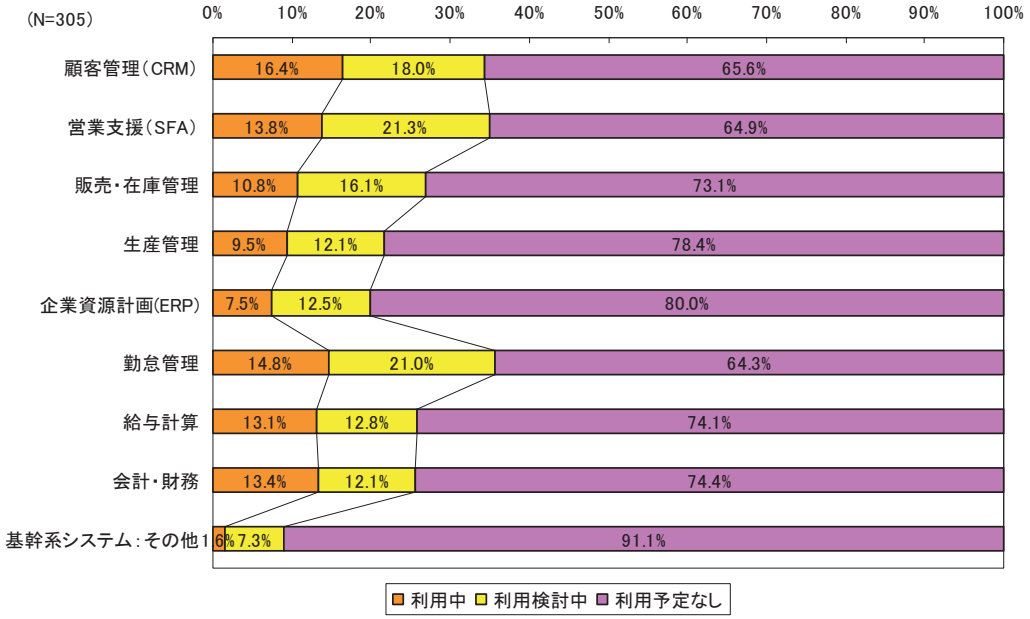
本アンケート調査におけるクラウド/SaaS の定義

クラウド：クラウド・コンピューティングを指すものとし、サーバ等が提供するサービスを、リソースを意識せずにネットワークを通じて使用できるモデルと定義する。SaaS（Software as a Service）や PaaS（Platform as a Service）等を包含したより広い概念とする。
SaaS （Software as a Service）：ユーザ側のコンピュータがソフトウェアを保有するのではなく、ソフトウェアの機能をサービスプロバイダがネットワークを通じて提供するモデルと定義する。ASP（Application Service Provider）の進化形で、利用者にとってより使い勝手が良く、利用価値が向上したものとする。

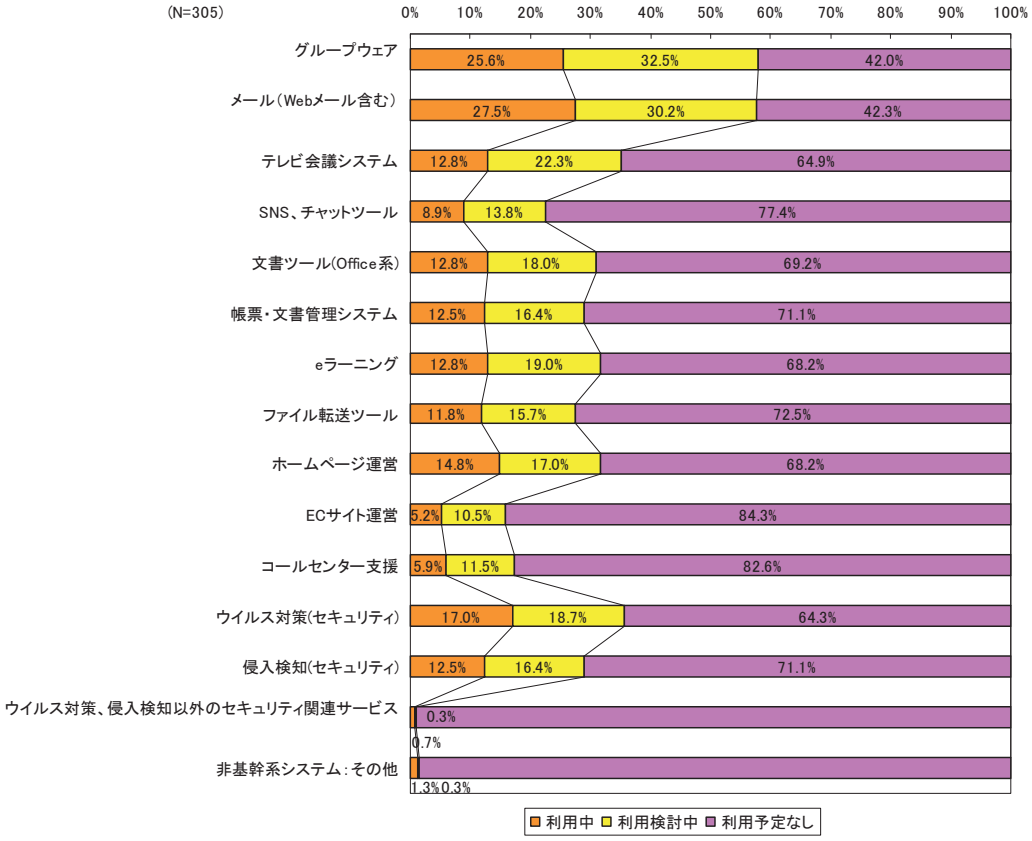
基幹系において利用率が高いサービスは顧客管理（16.4%）、勤怠管理（14.8%）等である。利用検討率としては営業支援（21.3%）、勤怠管理（21.0%）が高い。勤怠管理は基幹系システムの中でも業務に直結するサービスではないため、導入における障壁は他のサービスに比べ低いと考えられる。また顧客管理や営業支援については大手外資系事業者が中心となって国内でも広くサービスを提供しており、他の基幹系のサービスに比べて導入しやすい状況があると考えられる。

非基幹系では、グループウェアやメール等一般的なサービスにおいて、利用/利用検討率とも高い結果となった。

図表 3-6　クラウド/SaaS の各サービスの利用状況（基幹システム）



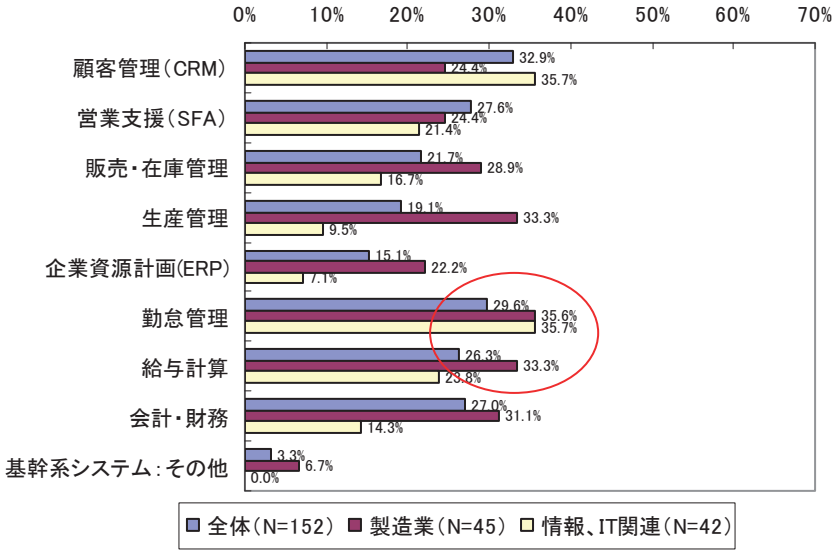
図表 3-7　クラウド/SaaS の各サービスの利用状況（非基幹システム）



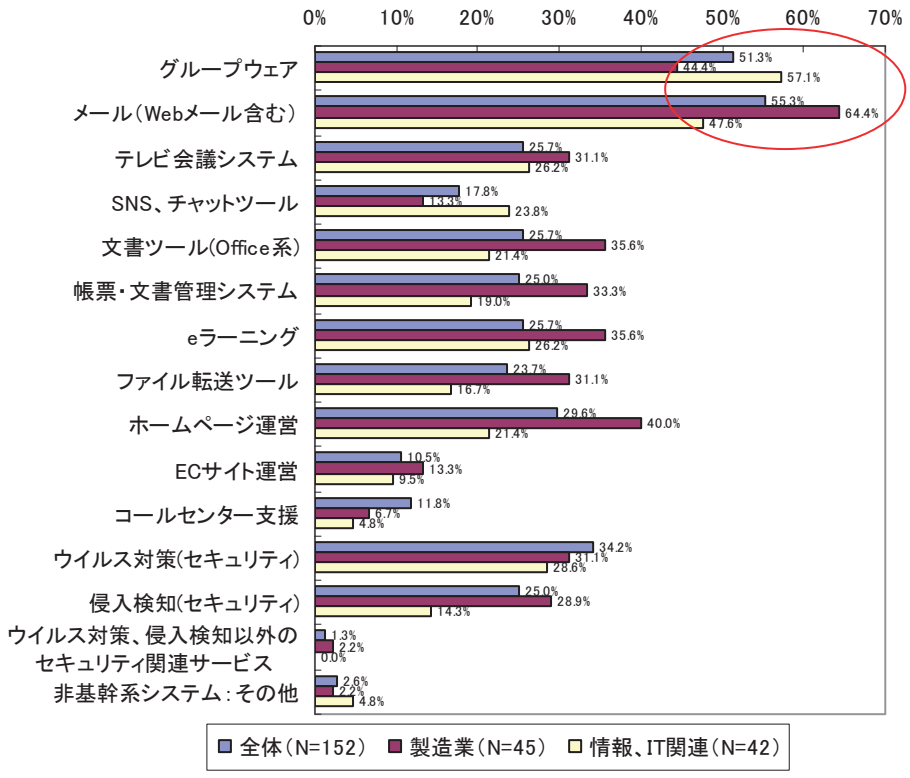
次に、利用者（152 名）のみを対象として結果を紹介する。

上記の利用動向を業種別に分析すると、基幹系の勤怠管理や、非基幹系のグループウェア等は業種に限らず利用率は高いが、それ以外では業種によって利用状況に差が見られる。全体的に製造業の方が利用率は高く、特に基幹系の販売・在庫管理や生産管理等、製造業特有の管理における利用が目立つ。情報・IT 関連では大半の利用率が低い結果となったが、1 つの可能性として、同様のシステムを自社で開発出来るため、外部環境への移行の必要性が低いという状況も考えられる。

図表 3-8　業種別クラウド/SaaS の各サービスの利用状況（基幹システム）



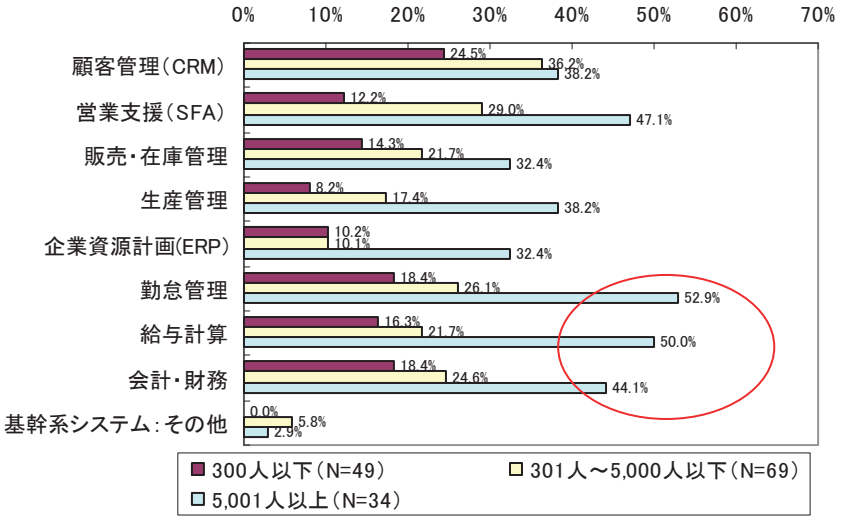
図表 3-9　業種別クラウド/SaaS の各サービスの利用状況（非基幹システム）



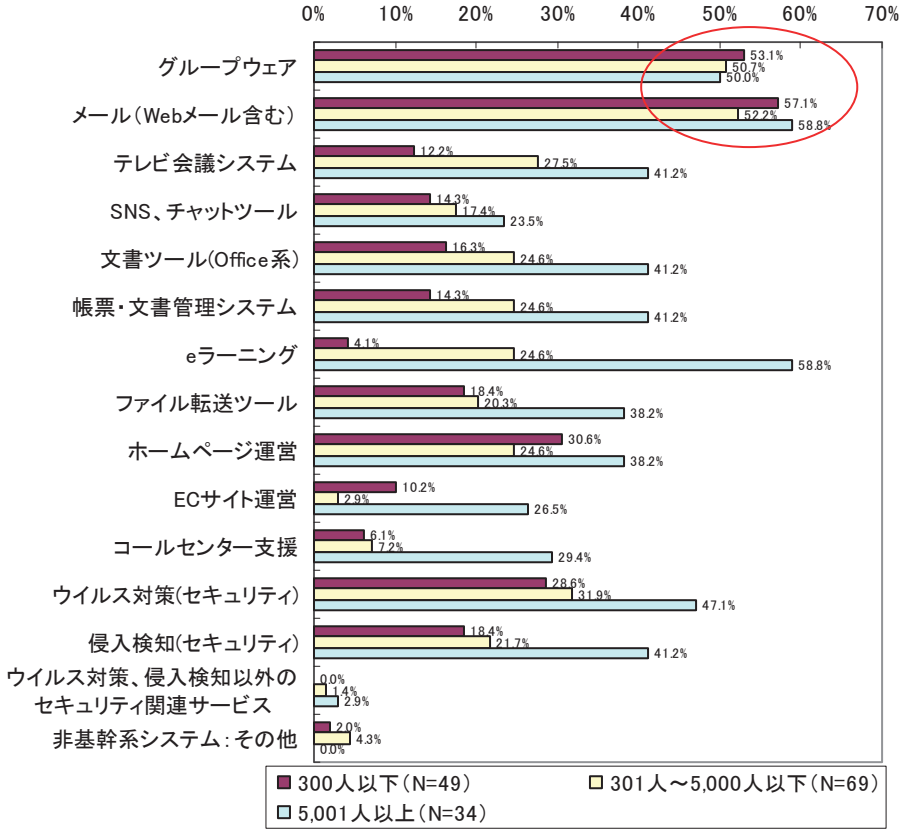
次に回答者の企業の従業員数、つまり企業規模別に分析を行うと、基幹系では、全体的に従業員数が多いほど利用率が高い結果となった。特に、勤怠管理や給与計算等では、回答した大企業（従業員 5,000 人以上）のうち、5 割以上が利用している。基幹系の中でも人事などの業務に直結しない管理では、クラウド/SaaS 導入への障害が低いと考え

られる。大半の非基幹系でも大企業の利用率の方が高いが、グループウェアやメール等、一般的なサービスでは、中小企業の利用率も高い。大企業が利用するサービスの幅が広いのに対し、中小企業では特定のサービスに集中した利用が進んでいる。

図表 3-10　従業員数別クラウド/SaaS の各サービスの利用状況（基幹システム）



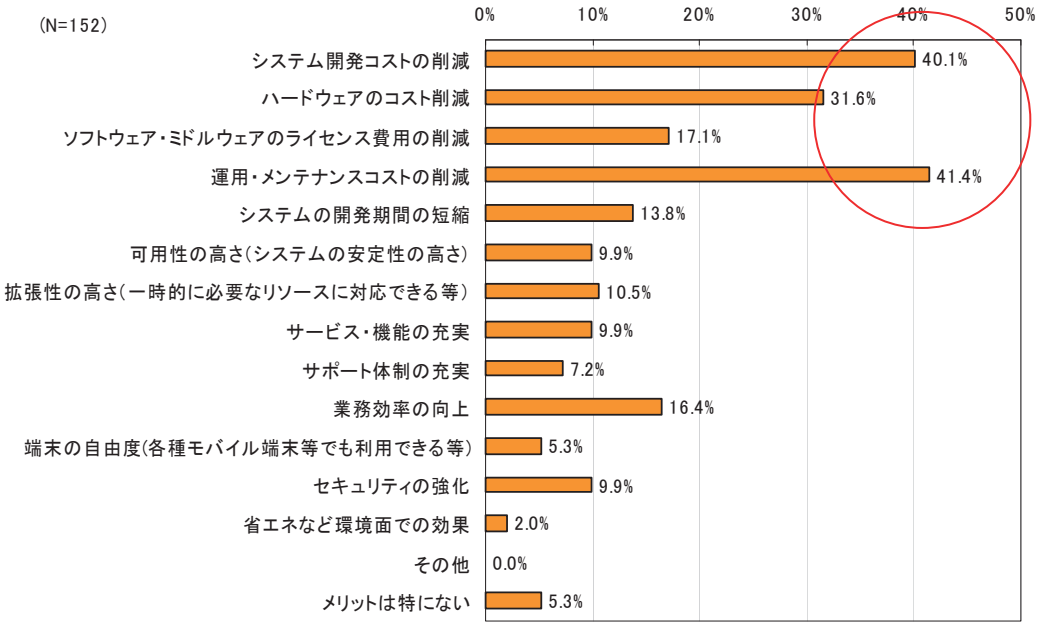
図表 3-11　従業員数別クラウド/SaaS の各サービスの利用状況（非基幹システム）



(4) クラウド/SaaS 導入のメリット

ここでは､利用者に対してクラウド/SaaS を導入したことによるメリットを聞いた。運用・メンテナンスコストの削減（41.4%）、システム開発コストの削減（40.1%）、ハードウェアのコスト削減（31.3%）の順に高い結果となり、現時点では、利用者のクラウド/SaaS 導入の主な目的はコスト削減にあるといえる。

図表 3-12　クラウド/SaaS 導入のメリット

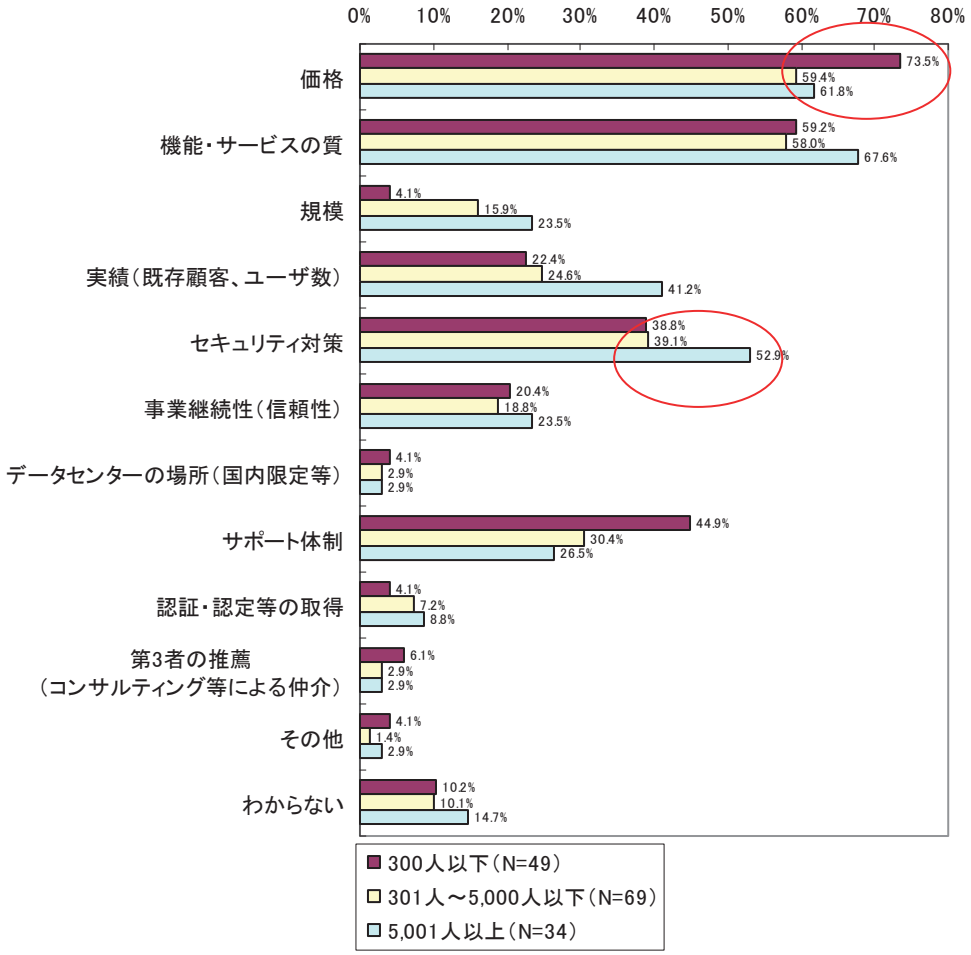


(5) クラウド/SaaS 専業者選定基準

クラウド/SaaS サービスを提供する事業者の選択について、企業規模別にその選定基準を分析した。クラウド/SaaS 専業者において、中小企業（従業員数 300 人以下）では、「価格」（78.5%）、「機能・サービスの質」（59.2%）、「サポート体制」（44.9%）の順に考慮されているのに対し、大企業（5,000 人以上）では、「機能・サービスの質」（67.6%）、「価格」（61.8%）、「セキュリティ対策」（52.9%）の順と、違いが見られる。

中小企業では、コスト削減等の目的でのクラウド/SaaS 導入が多く、機能・サービスの質よりは価格が重視されていると考えられる。また、サポート体制を重視するのは、自社内で情報システムの専門家等の担当者を設置するのが難しく、管理面も外部に依存したい状況もあると考えられる。一方、大企業では価格を考慮しつつも、機能面・サービスの質のメリットや付加的なセキュリティ対策等も重視しており、既存システムからクラウド/SaaS に移行することでコスト削減だけでなく、サービスレベルの維持・さらには向上を目指す方針が伺える。

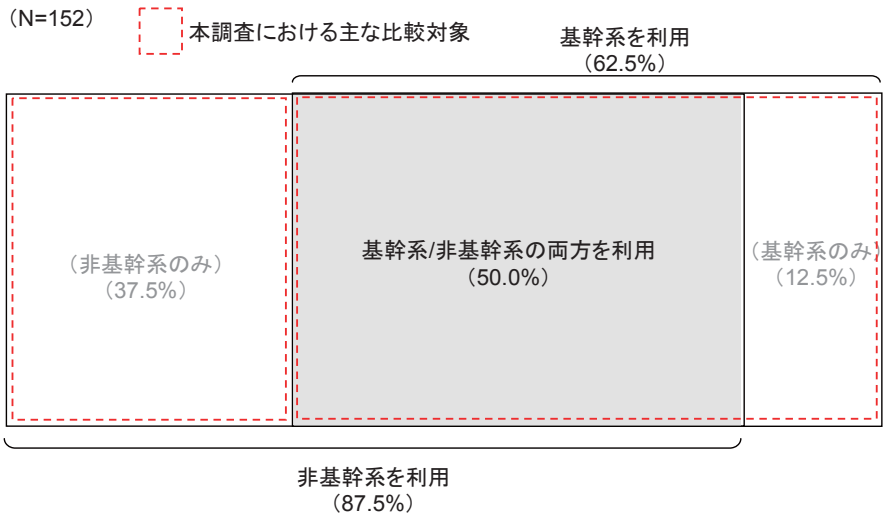
図表 3-13　従業員数別クラウド/SaaS 専業者の選定基準



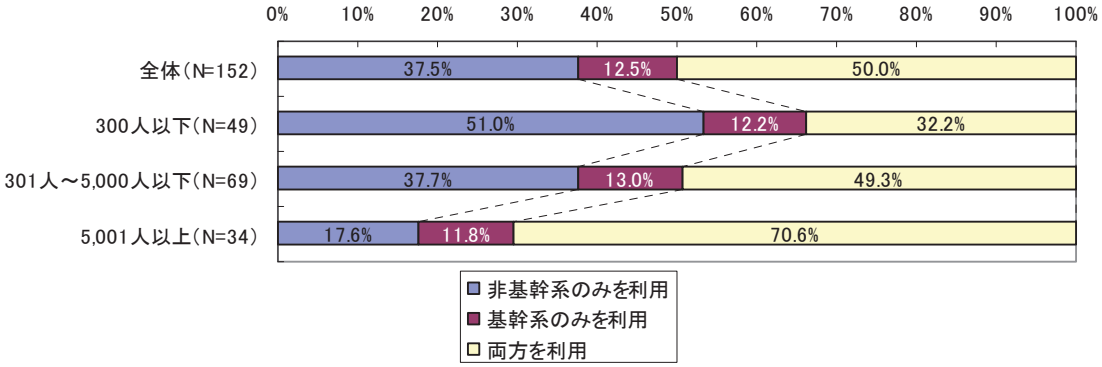
(6) 基幹系と非基幹系の利用状況（全体）

クラウド/SaaS 利用者のうち、基幹系のみを利用しているのは、12.5%、非基幹系のみを利用しているのは 37.5%となり、両方を利用しているのは 50.0%であった。さらに従業員数が 300 名以下の規模の小さい企業では、特に非基幹系のみの利用（51.0%）が目立ち、企業規模が大きくなるに従い基幹系の利用が進んでいる。

図表 3-14　クラウド/SaaS の利用状況の内訳



図表 3-15　基幹系と非基幹系の利用状況

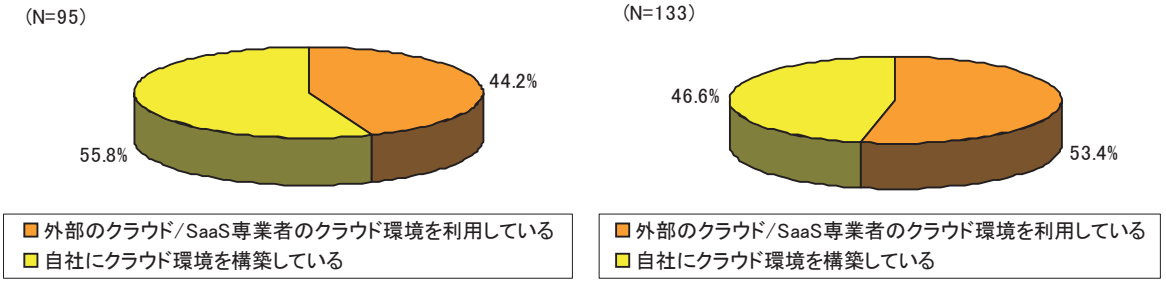


(7) 基幹系/非基幹系の利用状況（クラウド/SaaS の構築・利用形態）

クラウド/SaaS の構築・利用において、基幹系では「自社環境にクラウド環境を構築している」という回答（55.8%）が「外部のクラウド環境を利用している」という回答（44.2%）を上回ったが、非基幹系では逆の傾向（自社に構築：46.6%、外部の環境を利用：53.4%）が見られる。また、導入方法については、基幹系では導入に際し、クラウド/SaaS 専業者またはそれ以外の事業者の支援を受けたのは 60.3%、自社

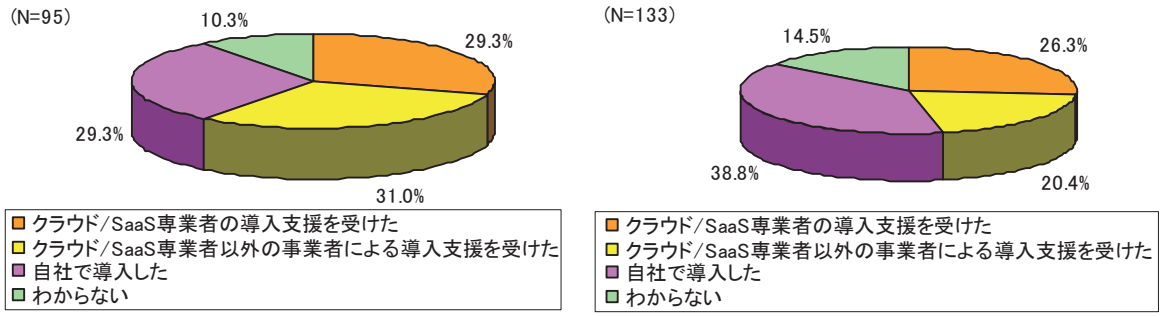
で導入したのが 29.3%であったのに対し、非基幹系では外部の支援を受けたのは 46.7%、自社のみで導入したのが 38.8%と差が見られる。基幹業務のサービスは自社内に留める傾向があり、さらに導入にあたっては事業者の支援を利用しており、非基幹系に比べて基幹業務のクラウド移行への難しさ、またはサービスの継続性確保に対する企業側の懸念が大きいと考えられる。また、基幹系の場合、既存システムにおいて特定のベンダや SIer が委託開発したものも多いため、そうした事業者自体が導入支援を行っている状況もあると考えられる。

図表 3-16　基幹系/非基幹系におけるクラウド/SaaS の構築・利用形態[18]



（基幹系）　　（非基幹系）

図表 3-17　基幹系/非基幹系におけるクラウド/SaaS の導入方法



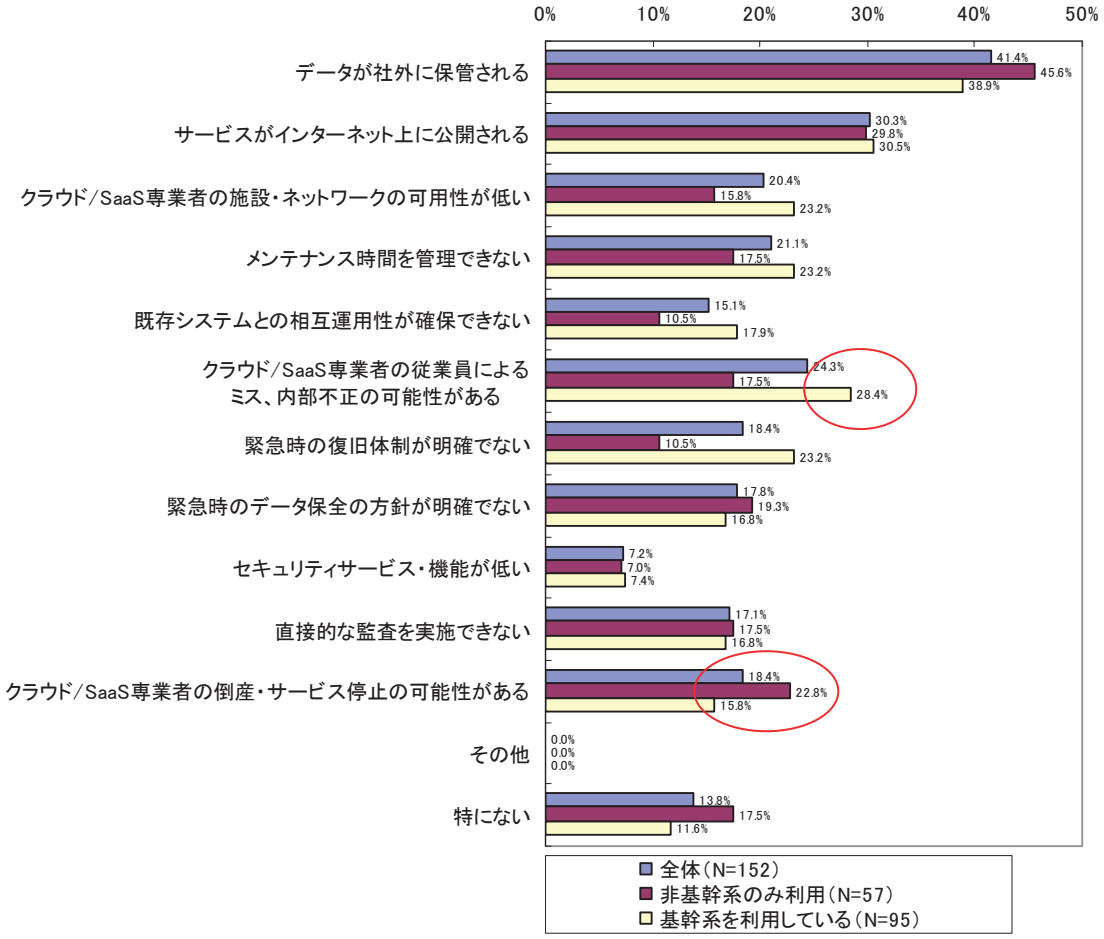
（基幹系）　　（非基幹系）

[18] 本設問ではクラウド環境を自社内に構築するプライベート・クラウドと、外部事業者の環境を利用するパブリック・クラウドの利用状況を把握する意図があったが、現在の企業のプライベート・クラウドの普及率が今回の調査結果に比べてかなり低い状況を考えると、「自社にクラウド環境を構築している」という状況が、厳密なプライベート・クラウドの範囲よりは広く捉えられている可能性がある。

(8) 基幹系/非基幹系の利用状況（クラウド/SaaS におけるセキュリティ上の課題）

全体として非基幹系のみの利用者に比べて、基幹系を利用している利用者の方がセキュリティ上の課題に対する認識は高い。特に、クラウド/SaaS 専業者のミス、内部不正（28.4%）、緊急時の復旧体制（23.2%）、ネットワークの可用性（23.2%）に関しては、基幹系の利用者の方が 10 ポイント以上高くなっており、サービスの可用性・信頼性が強く意識されている。一方で、クラウド/SaaS 専業者の倒産・サービス停止に関しては、非基幹系のみの利用者の方が高くなっており（22.8%）、事業者自体の財政的な事業継続性に不安がある、比較的小規模な事業者がサービスを提供している場合も多いと考えられる。

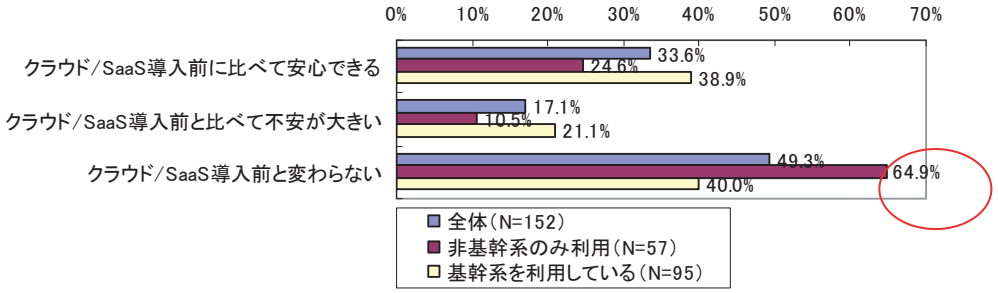
図表 3-18　基幹系/非基幹系利用者が抱くセキュリティ上の課題



(9) 基幹系/非基幹系の利用状況（求めるサービス）

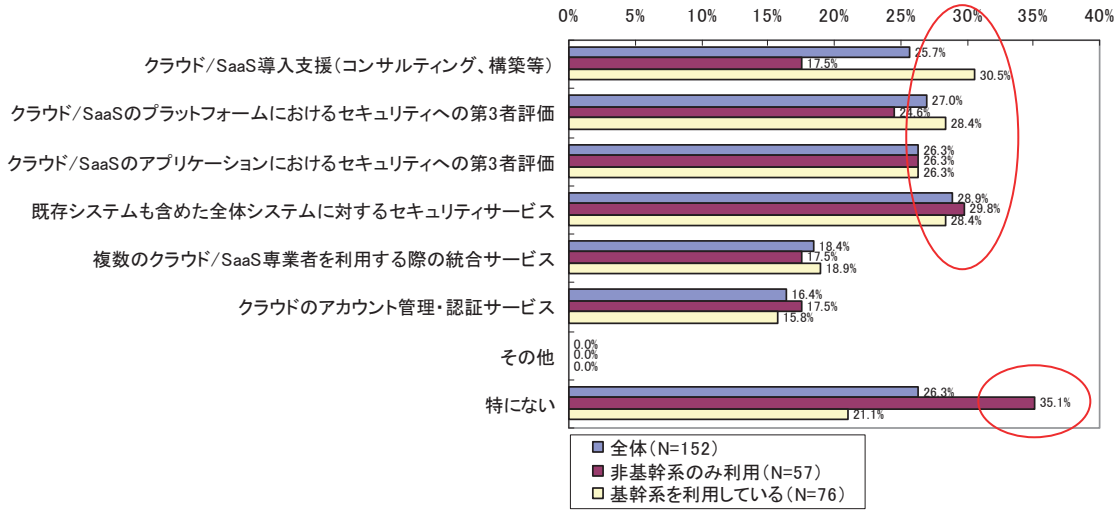
基幹系の利用者がクラウド/SaaS 導入後に持っている感想として、「安心できる」（38.9%）と「不安が大きい」（21.1%）のどちらの割合も非基幹系のみの利用者より高くなっており、結果によらずセキュリティに対する意識は高いと言える。一方で、非基幹系のみの利用者は「変わらない」という回答（64.9%）が基幹系の利用者に比べ 20 ポイント以上も高く、システムをクラウド/SaaS にしたことによるセキュリティへの影響は殆ど受けていない、または感じていないと考えられる。

図表 3-19　基幹系/非基幹系利用者が抱くクラウド/SaaS 導入後の安心感



同様にクラウド/SaaS 関連のサービスに関しても非基幹系のみの利用者に比べ、基幹系利用者の需要の方が全体的に高い。基幹系の利用者の需要が最も高いのは、既存システムも含めた全体システムに対するセキュリティサービス（28.4%）であるが、導入支援（31.5%）、プラットフォームに対する第 3 者評価（28.4%）では非基幹系に比べてポイントが高く、特に基幹系の導入において導入段階、プラットフォーム構築段階で課題を抱えている企業が多いと予想される。一方で、非基幹系では「特にない」（35.16%）との回答が最も多く、付加的なセキュリティサービスの需要は低いと考えられる。

図表 3-20　基幹系/非基幹系利用者が求めるサービス



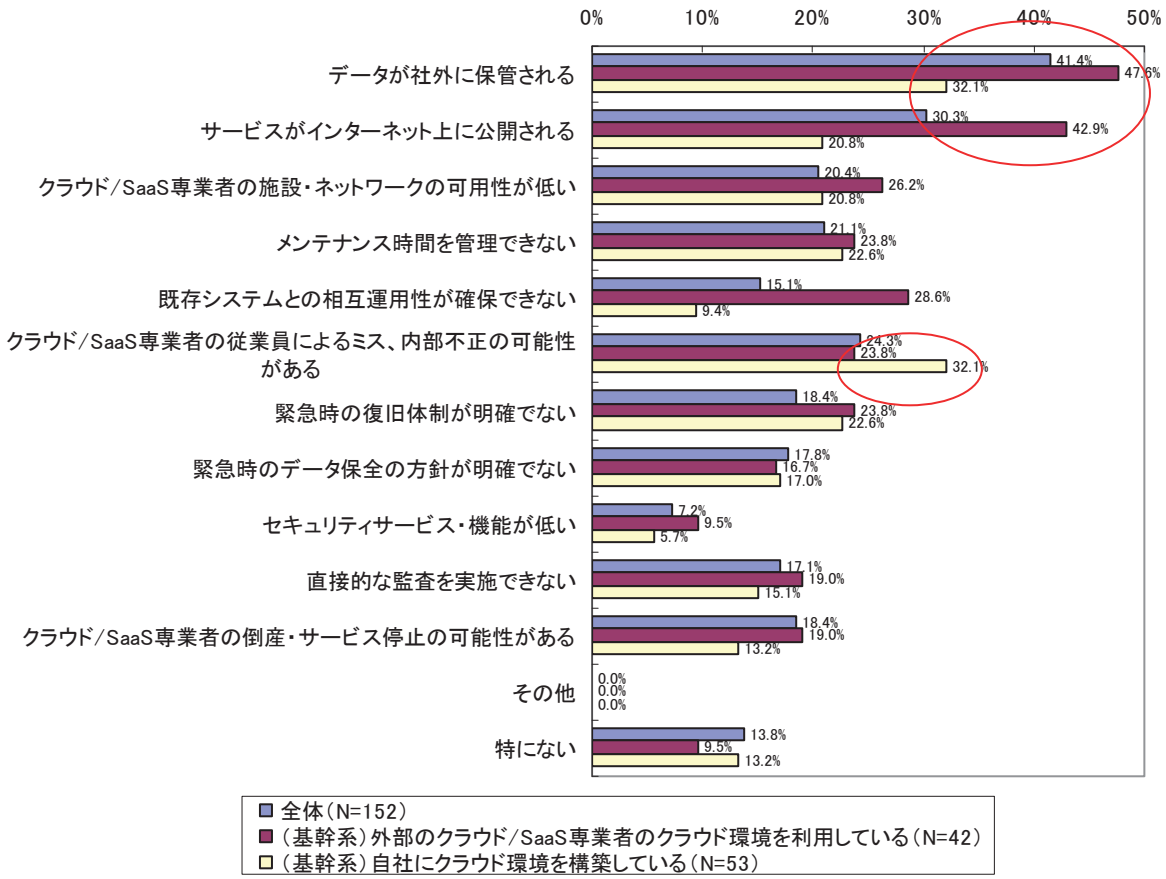
図表 3-21　基幹系/非基幹系利用者の傾向のまとめ

	非基幹系のみ （37.5%）	基幹系を利用 （62.5%）
規模	中小企業が中心	大企業が中心
業種	業種限らず	製造業等
導入方法	自社で導入	導入支援を利用
利用・構築形態	外部環境を利用	社内環境を利用
セキュリティ上の課題	事業者自体の事業継続性	事業者のミス/内部不正 緊急時の復旧体制 ネットワークの可用性
求めるサービス	目立ったニーズなし	全体システムのセキュリティに対する第 3 者評価 クラウド/SaaS 導入支援 プラットフォームのセキュリティに対する第 3 者評価

(10) 基幹系における外部環境/内部環境の利用状況

ここでは、基幹系利用者のうち、外部環境を利用する場合と自社内の環境を利用する場合を比較した。クラウド/SaaS のセキュリティの課題のうち、「データが社外に保管される」、「サービスがインターネット上に公開される」に関しては、自社環境利用者に比べ、外部環境利用者が 15 ポイント以上高い結果となった。自社環境を利用することで、情報を外に出すことへの不安はある程度解消されていると考えられる。他の項目についても外部環境利用者の方が大きな課題と感じている傾向が見られるが、「クラウド/SaaS 専業者の従業員によるミス、内部不正の可能性がある」の項目のみは、自社環境利用者の方が高い課題意識を持っている。この場合の「クラウド/SaaS 専業者」は「自社内のクラウド環境構築を委託した外部事業者」と考えられるが、彼らが自社内環境にアクセス出来る唯一の外部者であるために、彼らの不正行為に対して特に警戒が強くなっていると見られる。

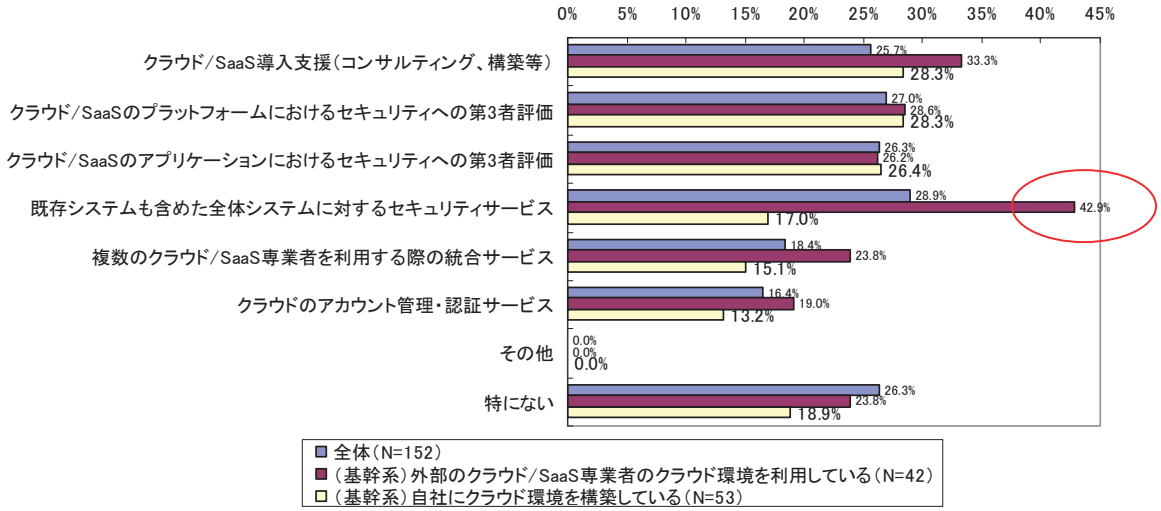
図表 3-22　外部環境/内部環境の利用者が抱くセキュリティ上の課題



外部環境利用者と、内部環境利用者が求めるサービスを比較したところ、全体的に外部環境利用者の方が各サービスへのニーズが高い結果となった。特に、外部環境利用者の「既存システムも含めた全体システムに対するセキュリティサービス」へのニ

ーズは 42.9%と圧倒的に高く、外部環境と内部環境の連携において支援を必要とする利用者が多いと考えられる。

図表 3-23　外部環境/内部環境の利用者が求めるサービス

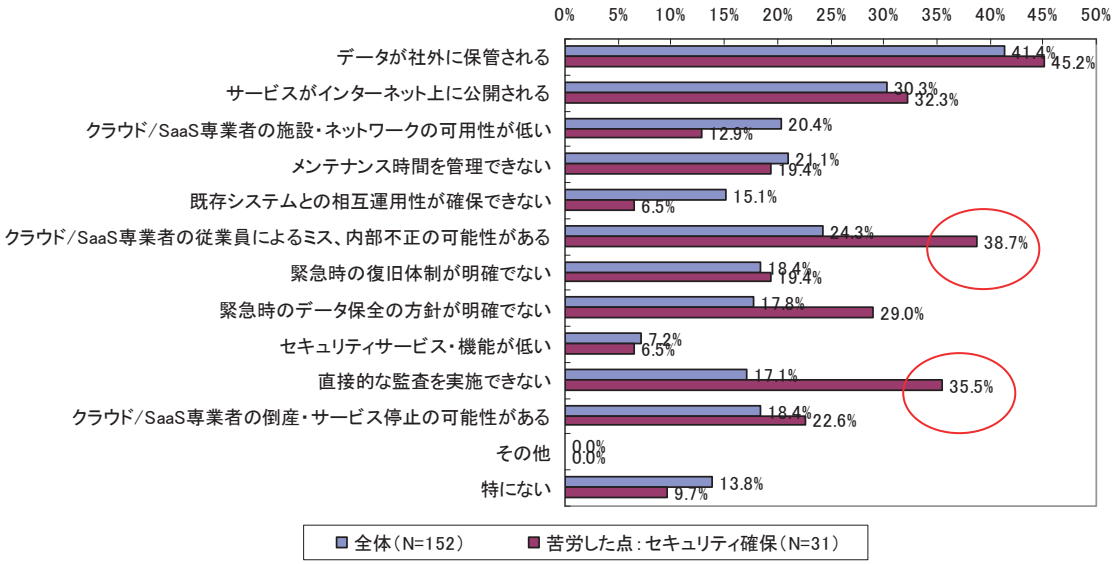


(11) セキュリティ意識が高い利用者の抱える課題

クラウド/SaaS 導入にあたり苦労した点として「セキュリティの確保」を挙げた回答者に対して、クラウド/SaaS のセキュリティ上の課題を聞いたところ、「データが社外に保管される」（45.2%）、「クラウド/SaaS 事業者によるミス、内部不正の可能性がある」（38.7%）、「直接的な監査を実施できない」（35.5%）となった。ちなみに、全体の回答との差が大きいのは、2 番目の「クラウド/SaaS 事業者によるミス、内部不正の可能性がある」（39.7%）と 3 番目の「直接的な監査を実施できない」（35.5%）、また「緊急時のデータ保全の方針が明確でない」（29.0%）となっている。

クラウド/SaaS という利用形態では、セキュリティ面はある程度事業者に依存せざるを得ない部分がある。回答者は比較的セキュリティへの意識が高いと予想されるので、物理的/技術的なセキュリティ対策についてはある程度理解していると考えられる。物理的/技術的なセキュリティ対策よりは、組織的な対策の部分の不透明さに不安を感じている状況が伺える。

図表 3-24　クラウド/SaaS 導入にあたり苦労した点として
「セキュリティ確保」を挙げた方が抱くセキュリティ上の課題

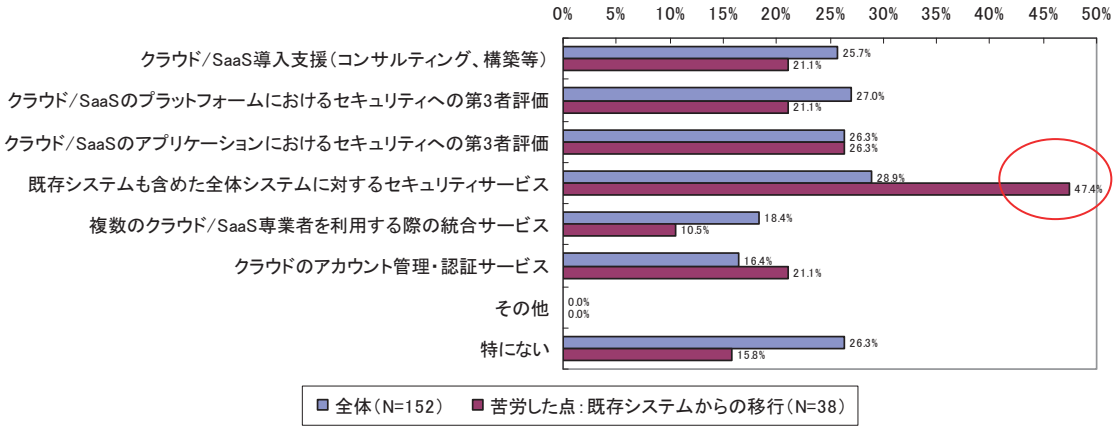


(12) セキュリティ意識が高い利用者が求めるセキュリティサービス

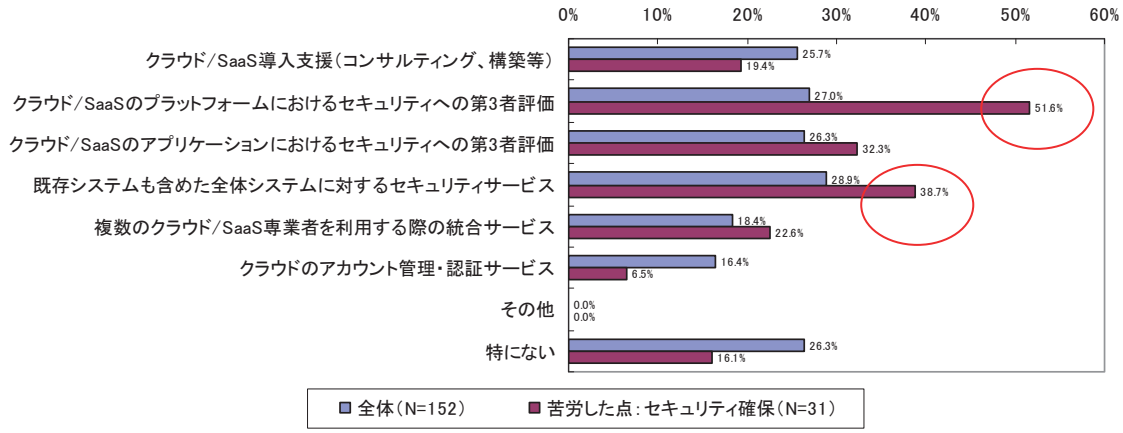
クラウド/SaaS 導入にあたり苦労した点として「既存システムの移行」を挙げた回答者に対して、求めるサービスを聞いたところ「既存システムも含めた全体システムに対するセキュリティサービス」へのニーズが 47.4%と全体の回答に比べて 20 ポイント以上も高い結果となった。既存システムがある場合、全体システムの中で相互運用性を確保されなければならないが、セキュリティ面においても同様の課題解決が求められていると考えられる。

また、同様にクラウド/SaaS 導入にあたり苦労した点として「セキュリティの確保」を挙げた回答者に対して、求めるサービスを聞いたところ、全体の回答に比べ「クラウド/SaaS のプラットフォームにおけるセキュリティへの第 3 者評価」が 20 ポイント以上、「既存システムも含めた全体システムに対するセキュリティサービス」が 10 ポイント以上高い結果となった。回答者はセキュリティ意識の高い利用者と考えられるため、個々の事業者やベンダの提供するセキュリティ対策は利用している場合が多いと考えられる。しかし、プラットフォームを含めた全体システムのセキュリティについては、それらとは別の専門的なサービスが求められているといえる。

図表 3-25　クラウド/SaaS 導入にあたり苦労した点として
「既存システムからの移行」を挙げた方が求めるサービス

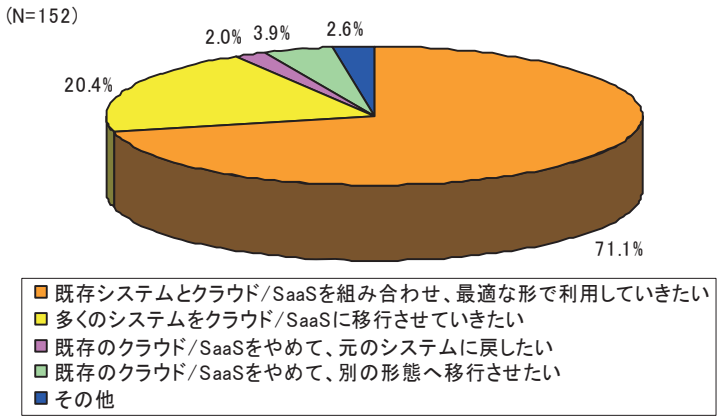


図表 3-26　クラウド/SaaS 導入にあたり苦労した点として
「セキュリティ確保」を挙げた方の求めるサービス



回答者が考える今後の情報システム利用における将来展望としては、「既存システムとクラウド/SaaS を組み合わせ、最適な形で利用していきたい」が 71.1%と最も高い結果となった。企業として、クラウドに移行すべきものとすべきでないものを見極めていくことが重要となると考えられる。

図表 3-27　情報システム利用における将来展望



3.2.2. 調査結果のまとめ

本調査結果によって明らかになった点を以下にまとめる。

(1) クラウド/SaaS の利用状況

回答者の企業におけるクラウド/SaaS 利用率は 2 割強､利用検討率も 2 割強であり、今後も一定の割合まで普及が進むと考えられる。

またシステム別には、非基幹系/基幹系とも大企業における利用が先行しており、中小企業ではグループウェアやメールといった特定サービスの利用に限定されている。

(2) クラウド/SaaS の利用形態

非基幹系のみを利用している企業では、外部のクラウド環境を利用する割合が高いのに対し、基幹系を利用している企業では自社内に構築したクラウド環境を利用する割合が高くなっている。本調査における「自社内のクラウド環境」は純粋な「プライベート・クラウド」を指すものではない可能性があるが、基幹系はプライベート・クラウド、非基幹系はパブリック・クラウドという一定の切り分けがなされていると考えられる。

また、基幹系利用者に絞って分析を行った結果、基幹系を外部環境、つまりパブリック・クラウドで利用する企業では、自社内環境で利用する企業に比べてデータを外に出すことへの不安が大きい傾向が見られた。

(3) クラウドに求めるメリット

クラウド/SaaS を利用することで得られるメリットはコスト削減効果との回答が圧倒的に多く、サービス内容やセキュリティ面では未だ事業者側のメリットに繋がっていない状況が伺える。一方で、特に大企業においてクラウド/SaaS 事業者の選定において、サービス内容、価格に次いでセキュリティ対策が重視されているという結果が得られた。事業者側にとっては、クラウド/SaaS のサービスにおいてセキュリティ面でどのような付加価値を出せるかが課題となっている。

(4) クラウド/SaaS におけるセキュリティへの不安

利用者が感じるセキュリティ上の課題として、最も多く挙げられたのが、「データが社外に保管される」､「サービスがインターネット上に公開される」という点であった。1.3.1.で示したように、クラウドにおけるセキュリティ上の課題としてデータの取り扱いが頻繁に議論されている通り、ユーザ側での不安もこの点に集中している。

またセキュリティ確保を重視している回答者は、「クラウド/SaaS 専業者の従業員によるミス、内部不正」､「直接監査が実施出来ない」といったコンプライアンスや監査等、技術面以外での不安も聞かれた。

(5) 利用者が求めるセキュリティサービス

クラウド/SaaS 導入時に既存システムからの移行に苦労したと回答した回答者では「既存システムも含めた全体システムに対するセキュリティサービス」へのニーズが高く、セキュリティ確保に苦労したと回答した回答者では「クラウド/SaaS のプラットフォームにおけるセキュリティへの第 3 者評価」へのニーズが高くなった。また基幹系利用者からは「クラウド/SaaS 導入支援」に対するニーズも高く、各社が利用するクラウド/SaaS の形態と利用状況によって様々なサービスが求められている。このようなサービスは、本報告書で議論されている「クラウド・インテグレーション」に求められているものと同様であると考えられる。

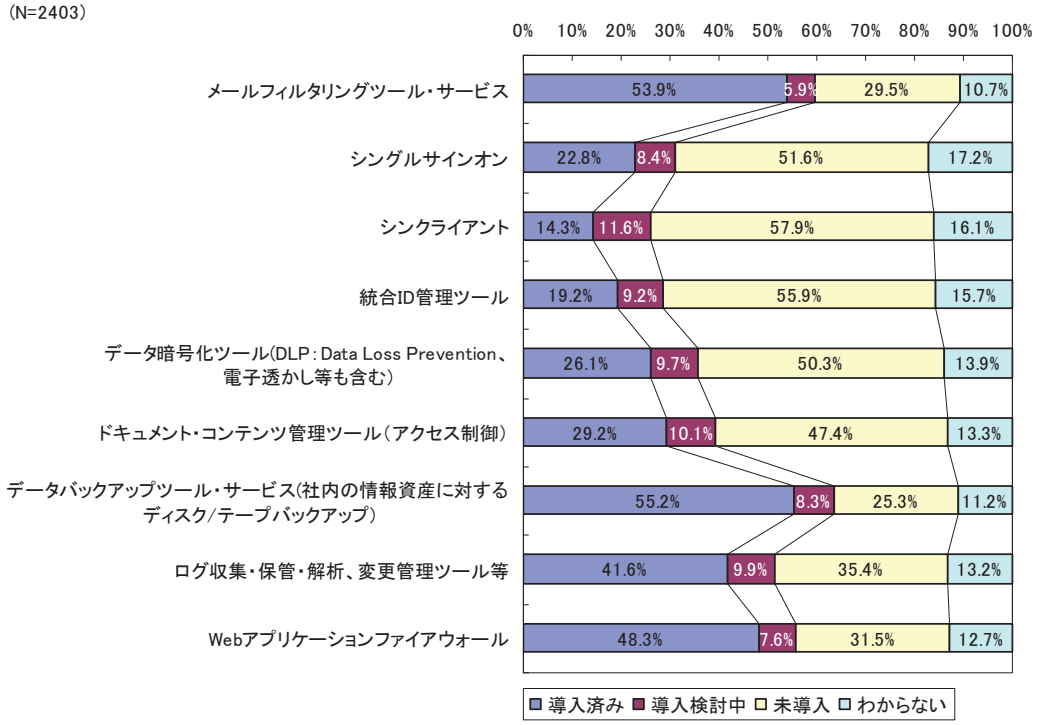
3.3. 情報セキュリティ製品・サービス導入状況

ここでは、クラウド/SaaS 利用動向とは別に毎年実施している情報セキュリティ製品・サービス導入実態と利用動向調査の結果を紹介する。本調査は 3.3.の第 1 次調査の一部として実施された。なお、本年度よりウィルス対策ツールやファイアウォール等、既に導入率が非常に高く、経年の変化が見られない製品・サービスは調査対象から除外し、比較的導入率が変化している製品・サービスに絞って調査を行った。

(1) 全体傾向

図表 3-28 に本年度の情報セキュリティ製品・サービスの導入率及び導入検討率の調査結果を示す。導入率が高いサービスは、メールフィルタリングツール・サービス（53.9%）、データバックアップツール（55.2%）、ウェブアプリケーションファイアウォール（48.3%）である。導入検討率は各製品・サービスにおいて大きな違いは見られないが、シンクライアントは 11.6%と比較的高い値となっている。

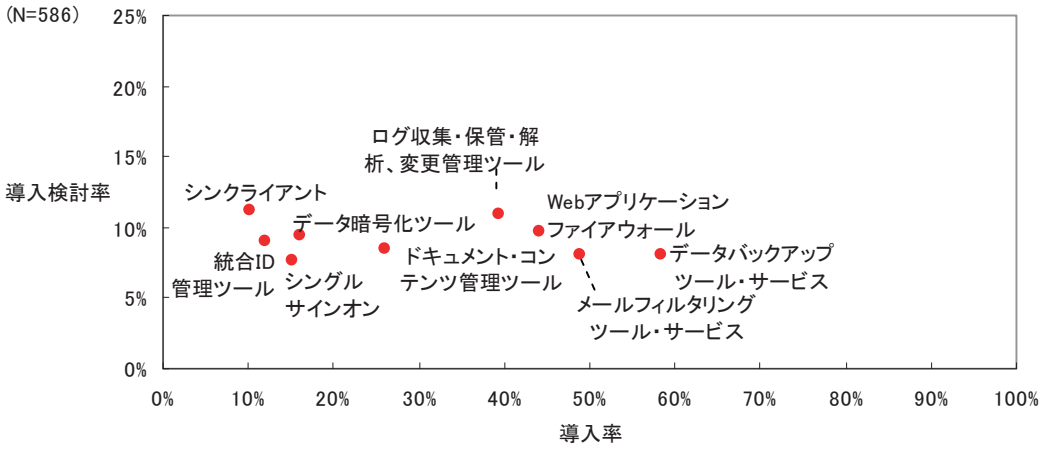
図表 3-28　情報セキュリティ製品・サービス導入状況



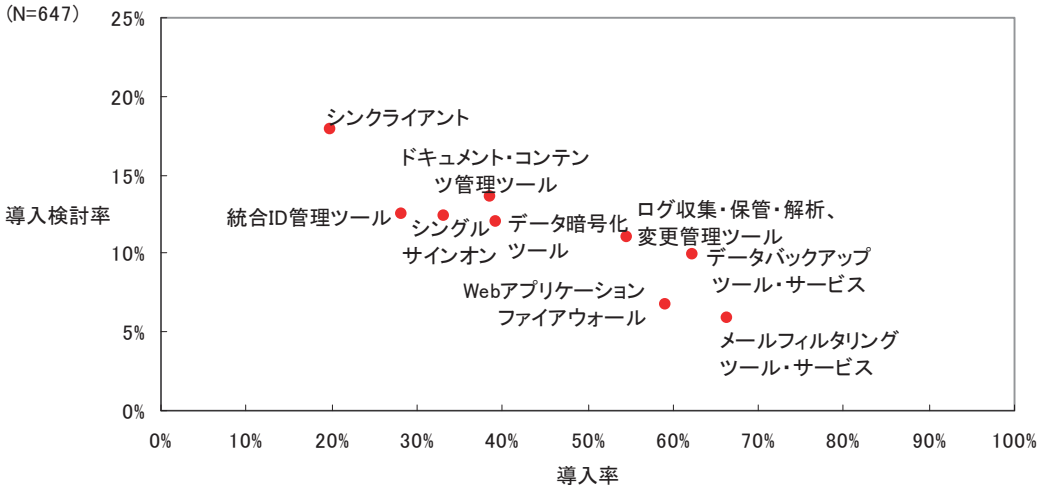
(2) 会社規模別

図表 3-29 から図表 3-31 に情報セキュリティ製品・サービスの導入状況を従業員数別に示す。全体的傾向として、従業員数 300 人以下の中小企業においては、導入率・導入検討率とも低く、従業員 301 人～5,000 人程度の中堅企業では、導入検討率が高くなり、5,000 人以上の大企業では、導入検討率は下がり、導入率が増加している。

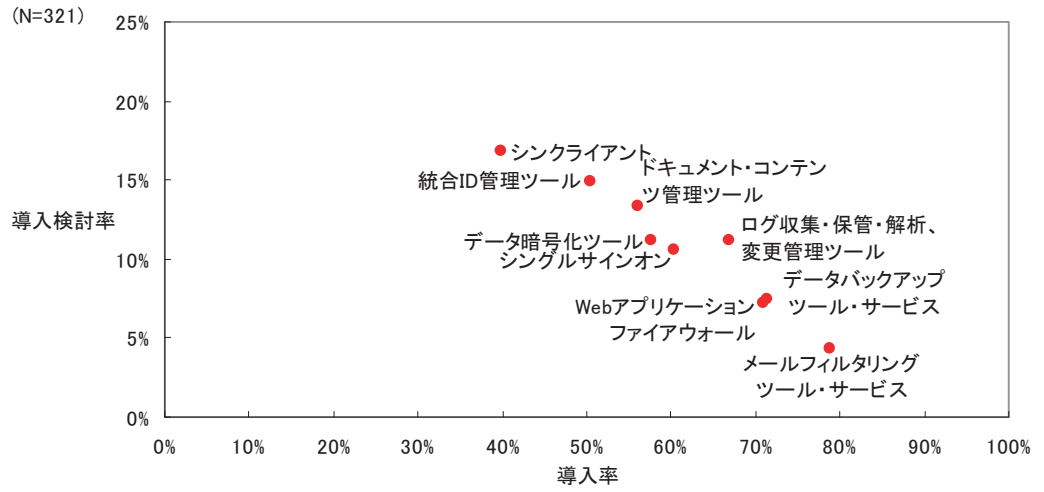
図表 3-29　情報セキュリティ製品・サービス導入状況（従業員 300 人以下)



図表 3-30　情報セキュリティ製品・サービス導入状況（従業員 301 人～5,000 人)



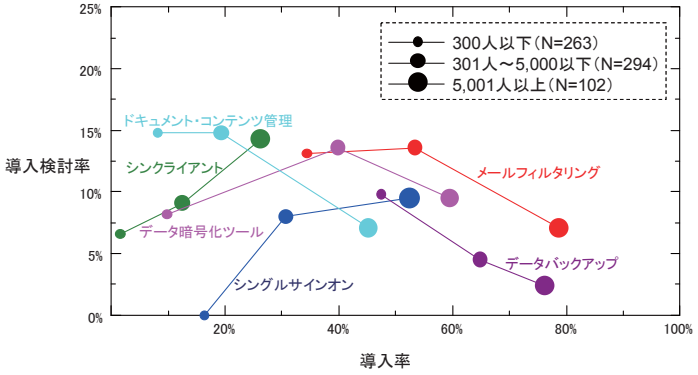
図表 3-31　情報セキュリティ製品・サービス導入状況（従業員 5,001 人以上)



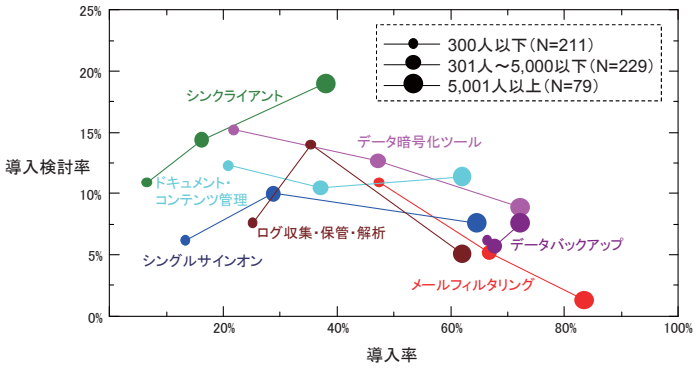
(3) 経年比較

図表 3-32 から図表 3-34 において、(2) の結果を 2007 年から 2009 年まで比較した。シングルサインオン、メールフィルタリング等のサービスは 2007 年段階では導入過渡期であったが、本年度の調査においては大企業において大半の企業で導入が進み、また中小・中堅企業でも徐々に導入/導入検討が進んでいる様子が窺える。また、シンクライアントに関しては、例年導入検討率が高い傾向にあるが、導入率が大きく増加することはないため、企業が導入に踏み切れない状況があると考えられる。

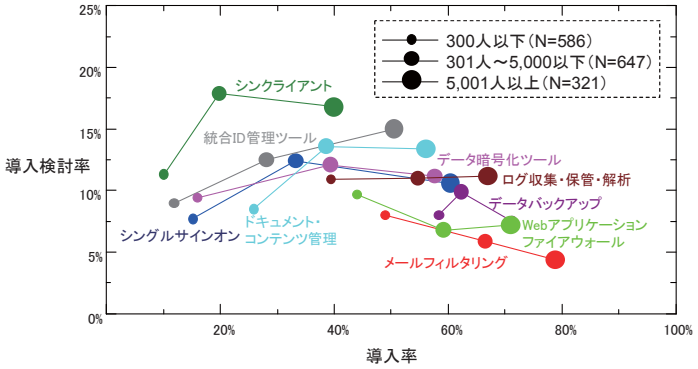
図表 3-32 情報セキュリティ製品・サービス導入状況（2007 年調査）



図表 3-33 情報セキュリティ製品・サービス導入状況（2008 年調査）



図表 3-34 情報セキュリティ製品・サービス導入状況（2009 年調査）



第４章　今後の情報セキュリティビジネスに向けた提言検討

4.1. 今後のクラウド/SaaS 普及シナリオ

4.1.1. 日本におけるクラウドの利用形態

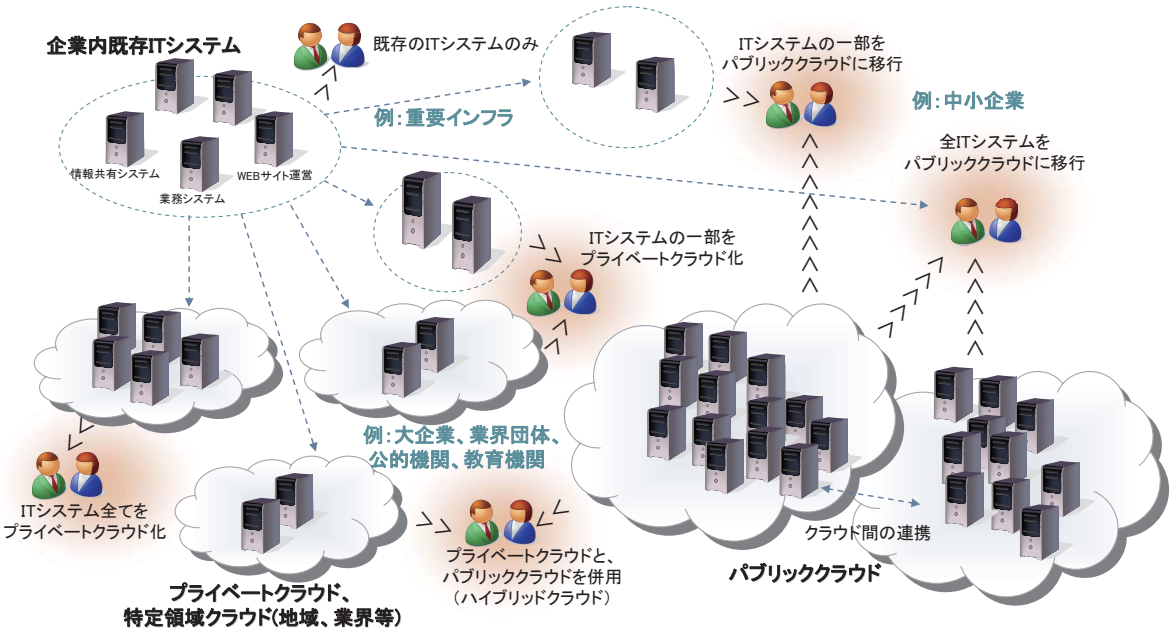
2009 年度の日本のクラウド市場は、米国大手事業者がサービス展開を先行する中、国内でもようやく多くの事業者がクラウド・ビジネスを打ち出し始めた年である。米国と比較した日本の大手ユーザ企業の特徴として、保有する IT システムのカスタマイズ性の高さ、サービスの信頼性やセキュリティに対するニーズの高さ等が挙げられることから、日本においてクラウド・ビジネスを展開する大手ベンダや SIer はプライベート・クラウドを中心とした展開に注力している。また、日本の中小企業ユーザにおいてもクラウドサービスの認知が進みつつあり、中堅 SIer では米国大手事業者のクラウドサービスのインテグレーションをサポートするビジネスを開始したり、分野に特化したソフトウェアベンダやサービスプロバイダの一部も、クラウド/SaaS への対応を図ったりする動きが見られる。

特に今後、企業によるクラウド・コンピューティングの利用形態は、各ユーザ企業に最適な形として多様化していくことが考えられる。

特に、日本においては、大企業において構築される基幹システムがユーザ毎にカスタマイズされた形態で提供されることが一般的であり、共通的なアプリケーションを提供するパブリック・クラウドにはそぐわない。そこで、基幹システムの多くはプライベート・クラウドを利用し、一部のシステムのみをパブリック・クラウドに移行させるハイブリッド形式が主流になると考えられる。一方、中小企業など、自社システムの作り込みの部分が少ない企業や、コスト制約の厳しい企業においては、共通的なアプリケーションを比較的安価に利用できるパブリック・クラウドへのニーズが高まるものと思われる。また、企業規模を問わず、特定領域（業界、自治体）向けのクラウドを利用する可能性もある。日本では、サービス利用にあたり、その信頼性を事業者のブランドバリューや実績で評価する傾向も強いことから、中小企業におけるクラウドの普及は、米国に比較してやや遅れているのが現状であるが、大手事業者の本格的なクラウド・ビジネス参入や、既存クラウド/SaaS 事業者による実績の積み重ねによって、徐々に市場開拓が進展すると考えられる。

市場の開拓に伴い、パブリック・クラウドにおいては、複数事業者が連携し、プラットフォームやデータの共通化やサービス間の相互利用・認証が促進される可能性もあり、さらなるユーザの利便性向上や導入コストの低減により、市場拡大が促進されることも考えられる。

図表 4-1　クラウド/SaaS の普及シナリオ



資料：三菱総合研究所作成

以上の傾向を踏まえると、日本におけるクラウド・コンピューティングの利用形態は以下のパターンが想定される。

（ア）　パブリック・クラウドを中心に利用

主に非基幹系など情報系システムを対象として、パブリック・クラウドを中心に利用する形態。特に、中小企業や新規に起業する企業、システムの新規導入の場合等に有効である。

（イ）　プライベート・クラウドとパブリック・クラウドのハイブリット利用

基幹系システムはプライベート・クラウド中心、非基幹系システムはパブリック・クラウド中心のハイブリッドで利用する形態。特に日本においては主流になると考えられ、日本の大手ベンダや SIer にとって新たなビジネス戦略が必要となる領域である。また、米国の主要クラウド/SaaS 事業者も、日本の事業者とのパートナー連携を深め、ユーザ層の拡大を図ると考えられる。ユーザ企業によってハイブリッドの最適値は異なり、既存の IT 資産、求められるセキュリティレベル、運用・メンテナンスコスト、システム改修時期等、様々な要素が判断基準となる。

（ウ）　プライベート・クラウドを中心に利用

企業のシステムの殆どを基幹系システムで占める企業や、クローズドなシステムが多い重要インフラ分野の企業等、非常に特殊な分野に限定された中で、システムの一部をプライベート・クラウドに移行する形態。もともとそのようなシステム形態である企業は、システム稼働の信頼性や保有するデータの機密性を非常

に強く重視する企業に多いと見られるため、クラウドに移行するメリットがないと導入は進まないと考えられる。

4.1.2. クラウド利用時のセキュリティに対するニーズと市場構造変化

以上のような形態でクラウド・コンピューティングが利用されるにあたり、クラウド・コンピューティングにおけるセキュリティの在り方は変化し、それに伴い IT 市場の構造変化が起こることが予想される。

パブリック・クラウドを中心として利用される場合は、ユーザ企業のセキュリティレベルが必ずしも高くない場合があるため、ユーザ企業側においては規模の経済で自社では実現できないセキュリティレベルのサービスを享受することが可能となる。ユーザ企業においては、セキュリティ対策の多くを外部事業者に任せることが可能となり、自身で行うべきセキュリティ対策として自社に残る部分が変化していくことも想定される。一方、別の見方として、クラウド/SaaS 事業者に要求するセキュリティレベルが高い一部のユーザ企業によって、クラウド/SaaS 事業者側にある程度のセキュリティレベルを確保したサービス提供の義務と責任が生じるため、事業者のセキュリティレベル向上が促進される効果もある。

いずれの場合も、クラウド/SaaS 事業者自らがセキュリティサービスを飲み込み、セキュリティサービス事業者としての一面も有することとなり、セキュリティサービスをユーザ企業に対して直接提供するビジネスを行う事業者にとってはビジネス戦略の変化を迫られる状況となりうる。セキュリティサービス事業者としては、自身がクラウド/SaaS 事業者としてより付加価値の高いセキュリティクラウドサービスを展開する他、クラウドを利用するユーザ企業に残されたセキュリティ対策もしくはクラウド利用時に求められる新たなセキュリティ対策の支援を行うか、クラウド/SaaS 事業者が対応できないセキュリティ対策もしくはセキュリティサービスについてクラウド/SaaS 事業者に対して支援を行う形態にシフトせざるを得ない。但し、必ずしも市場全体が縮小する訳ではなく、クラウドの普及に伴い、求められるセキュリティサービスの内容とビジネスの対象が変化する可能性があるという言い方が正しいだろう。

プライベート・クラウドとパブリック・クラウドの併用であるハイブリッド利用は日本の主流になると考えられるが、クラウド利用時の一般的なセキュリティの確保が必須であることに加え、ユーザ企業における既存システムも含めた全体システムとしてのセキュリティレベルの評価とセキュリティの確保、或いはサービス連携時のデータ安全性の確保や認証の統合が新たなセキュリティニーズとして求められるようになるだろう。最適なシステムバランスとセキュリティの確保という点では、ユーザ企業の要求仕様やシステム構造を熟知する大手ベンダや SIer にとって強みになることは間違いない。しかし、クラウドという新たな領域におけるセキュリティの確保という点では、技術的・運用的に新たなノウハウや知見が必要となるため、提供サービスの内容については革新と変化が求められる。また、従来以上にハードウェア売りではなく、コンサルティングやアプリケーション、ク

ラウド・インテグレーション等サービスで収益を得るモデルにシフトせざるを得ない状況となるだろう。また、パブリック・クラウド部分については、他のクラウド専業事業者による安価なサービスに代替される部分が増えると考えられ、オープン戦略でパブリック・クラウド/SaaS 事業者を取り込み連携部分で付加価値を取るのか、あくまでもクローズド戦略で自社サービスに取り込むのかの戦略性も見極めなければならない。一方で、第三者的立場による客観的な視点でのセキュリティ評価に対するニーズも高まると想定されるが、完全な第三者事業者によるセキュリティ評価サービスは、ユーザ自身もコストをかけづらい領域であり、事業者にとっても従来単体ではビジネスとして確立しづらい性質を持つ。ユーザに対し法的・制度的な責任が課せられない限り、内部を知る大手ベンダや SIer によるセキュリティ評価に留まる可能性は高いと考えられ、逆に言えば、大手ベンダや SIer にとっても、セキュリティレベルの評価ニーズにある程度応えられることは、サービス展開上の強みになるだろう。

プライベート・クラウド中心の利用形態が予想されるユーザ企業層においては、もともと非常に高いセキュリティレベルが要求されているため、移行そのものが当面進まないと予測されるが、プライベート・クラウドに移行した場合も、従来通りユーザの事情に通じた大手ベンダや SIer 等がセキュリティ確保を行う形態が継続するだろう。それ以外の事業者にとって参入障壁が高いため、クラウドの普及によって急速な市場構造変化は考えづらい領域であるが、この場合も、クラウドという形態に対応したセキュリティサービスの変化が求められることは間違いなく、さらにシステムの継続稼働やデータ保全に関する信頼性確保が重要になるだろう。

4.2. クラウド/SaaS 時代における情報セキュリティビジネスに向けた提言

本調査によって実施した日米のクラウド/SaaS 事業者に対するヒアリング・文献調査より、有望なクラウド/SaaS 市場ビジネスのポイントは以下が挙げられた。

図表 4-2　有望なクラウド/SaaS ビジネスのポイント

提供サービスにおけるセキュリティの確保	・クラウド/SaaS事業者から面倒を看られないのはクライアントセキュリティに係わる部分。 ・米国の主要な事業者においては、セキュリティ機能の提供に関し、自前で行う事業者と、提携事業者の協力を得る場合といずれのケースもある。
セキュリティに対する付加価値としてのユーザニーズ	・基本的には、社会認知が進む中で、セキュリティより価格に流れる方が現実的。 ・基幹系は中で持ち、情報系は外に出すという意向は、大企業だけではなく中小企業でも同じ印象。 ・セキュリティ機能はオプションとしての提供になるのではないか。 料金体系や手続きの一本化による判断のしやすさがメリットとなる。 ・高いセキュリティや信頼性を求める業界においては、信頼性担保のための第三者の認証等へのニーズはある。
クラウド/SaaS事業者としての差別化ポイント	・ユーザに対するビジネス上の付加価値の提供が重要。クラウドの最適な提供方法は様々。 ・ユーザの個別ニーズの差分の吸収と差別化のバランスによって、魅力的なサービスを提供。 ・ユーザから顔の見える立場として、ユーザに対する信頼感の提供が最も重要。 顧客との密なコミュニケーション、実績、ユーザの状況に応じたサービスの提供等。
売り方のポイント	・サービスの形態がクラウド/SaaSに変化しただけ。ユーザにとって新しい言い方でハードルが高まっている面もある半面、新しいサービスだからやるというユーザもあり、うまい移行が必要。 ・最初は、安全対策を含めて提供できる料金設定を行い、安全性にニーズが無かった場合は、機能性を高める方向性で料金設定を行う。いったん価格を下げると上げられない。
クラウド/SaaS移行のポイント（小規模事業者）	・初期投資が必要だが、すぐに儲けにならないことが問題。電算センターの使用、契約の問題、売上フローを描ききれない等の課題がある。協力会社の力を借りず、自社内のマンパワーでやることを検討した。 ・当初、サービスは、万一売れなくても自社で使えるアプリケーションとして構築した。

また、クラウド/SaaS に対するニーズとして、ユーザ企業に対するアンケート調査からは以下が示された。

図表 4-3　クラウド/SaaS ビジネスに対するニーズ

ターゲットユーザ	・電気通信業、金融・保険業、情報、IT関連企業など、ITを利用する機会の多い企業、大企業での利用率が高い。製造業は、特に基幹系の販売・在庫管理や生産管理等。基幹系では、大企業ほど利用率が高い。
有望なサービス	・基幹系は、大企業が多く利用し、プライベートクラウド形態で、導入時の事業者の支援を必要とする。 ・基幹系/非基幹系の両方を利用している利用者はセキュリティ上の課題に対する認識は高い。 ・セキュリティ意識の高いユーザについては、 - 既存システムも含めた全体システムに対するセキュリティサービス - クラウド/SaaSのプラットフォームにおけるセキュリティへの第3者評価

これらの調査結果を踏まえ、図表 4-4 において、クラウド時代のセキュリティビジネスモデルを、セキュリティの提供形態（インテグレーションが主形態 / セキュリティが主形態 / それ以外の新しい形態）及び提供タイプ（直営=SaaS / 直営＋卸売=SaaS 主体＋PaaS / 小売店=PaaS 主体+SaaS）別に分類した。これらのビジネスモデルのうち、クラウドの普及に伴うセキュリティの在り方の変化、そしてそれに伴う市場構造の変化の予測から、特に JEITA 会員企業にとって有望なセキュリティビジネス展開の方向性として以下が考えられる。

(1) システムインテグレーションやセキュリティサービスのクラウド化
（クラウド・インテグレーション）
(2) 複数のクラウド/SaaS 事業者を束ねたクラウド・インテグレーション
(3) エンドユーザに対する新たなセキュリティサービスの提供
(4) クラウド/SaaS 事業者に対する専門セキュリティサービス

図表 4-4　クラウド時代の有望なセキュリティビジネスモデル

セキュリティの提供形態	提供タイプ	現在の主な事例	SIerのセキュリティビジネスモデル	ビジネス性	実現時期	
（Ⅰ） クラウド/SaaS インテグレーション （従来のSIのクラウド化） にセキュリティ機能を付加	(A)直営モデル SaaS専業	一般的なASP事業者	SIerが主体となってシステムインテグレーションをクラウド/SaaS化（プライベートクラウド）	○	近	(1)
	(B)直営＋卸売モデル SaaS主体＋PaaS	Salesforce.com 等 米国大手クラウド事業者	SaaS事業者のバックでPaaSを提供 SaaS＋PaaS提供時にクラウドインテグレーション	△ △	近～遠 遠	
	(C)小売店モデル PaaS主体＋SaaS	国内大手SIer	SIerがPaaSとしてSaaS専業者と連携して（束ねて）クラウドインテグレーションを提供（パブリッククラウド）	★	近～遠	(2)
（Ⅱ） セキュリティサービスの クラウド/SaaS化	(A)直営モデル （Sec-）SaaS専業	セキュリティSWベンダ セキュリティサービスプロバイダ	SIerのセキュリティサービスをSaaS/クラウド化	○	近	
	(B)直営＋卸売モデル （Sec-）SaaS主体＋PaaS	Symantec等 セキュリティSaaS事業者	セキュリティSaaS事業者のバックでPaaSを提供 SaaS＋PaaS提供時にクラウドインテグレーション	× △	近 近	
	(C)小売店モデル （Sec-）PaaS主体＋SaaS	大手SIer、ISP	SIerがPaaSとしてセキュリティSaaS専業者と連携して（束ねて）クラウドインテグレーションを提供	★	近	
（Ⅲ） クラウド/SaaS時代の 新たなビジネスモデル	(a)クラウド時代の新たなセキュリティに関するサービス	セキュリティSWベンダ セキュリティサービスプロバイダ	エンドユーザに対しクラウド/SaaS事業者が提供しづらいセキュリティサービスを提供	○	近～遠	(3)
	(b)クラウド/SaaS事業者に対する専門セキュリティサービス	セキュリティSWベンダ セキュリティサービスプロバイダ	クラウド/SaaS事業者に対するセキュリティサービスを提供	○	中～遠	(4)

★ 国内大手SIer/ベンダにとって有望　○ 有望　△ やや有望　× 有望でない

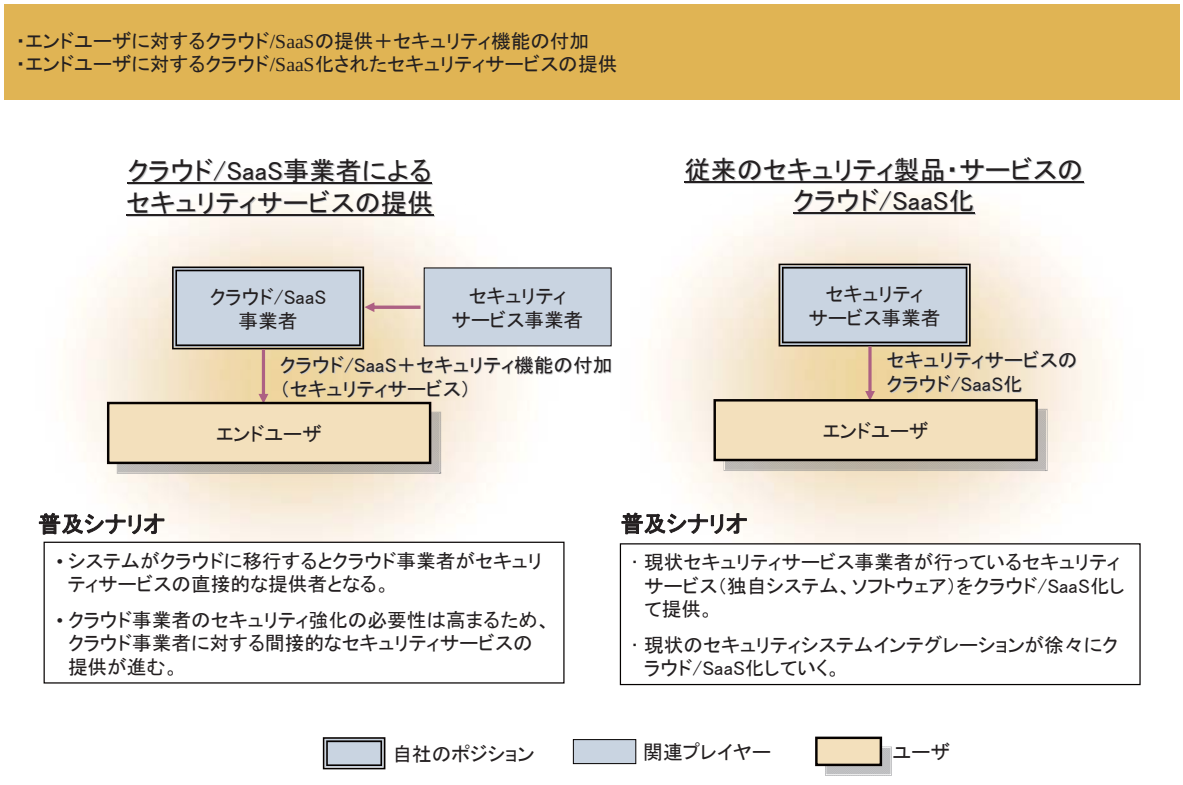
(1) システムインテグレーションやセキュリティサービスのクラウド化

大手ベンダや SIer が従来中心としてきたビジネスドメインについて、インテグレーションの形態がクラウドに変化するものであり、従来ビジネスの延長線上にあると言える。

日本のユーザ企業においては、システムのカスタマイズ性の高さやセキュリティやシステムの信頼性に対するニーズが強いことから、システムインテグレーションを外部事業者に依存する傾向が強い。そのため、安価で手軽に利用可能なクラウドサービスが普及したとしても、自身で一から導入するのは一部の簡易なサービスに限定され、システムの大半は従来から取引のある大手ベンダや SIer を通じた導入になると考えられる。そのため、従来のシステムインテグレーションから、徐々にクラウド・インテグレーションに移行していく形態が自然であると想定される。その際には、クラウドという新たな技術に対して、従来型のセキュリティ確保に加え、クラウド化されることによって生じるデータ保全や分散するリソースを活用する中で新たな形態のセキュリティの確保が必要となる。また、日本人独自の文化として、きめ細かいサービスやシステムのクオリティの高さに対するニーズが強いため、ユーザの要望に対応可能で、信頼感を確保し続けることが可能なサービス事業者が生き残っていくと考えられる。

また、クラウドサービスは中小企業にも導入しやすい形態であるため、手軽なクラウドサービスを契機としたクラウド導入支援サービス等によって、新たな市場を開拓できる可能性がある。

図表 4-5　システムインテグレーションやセキュリティサービスのクラウド化

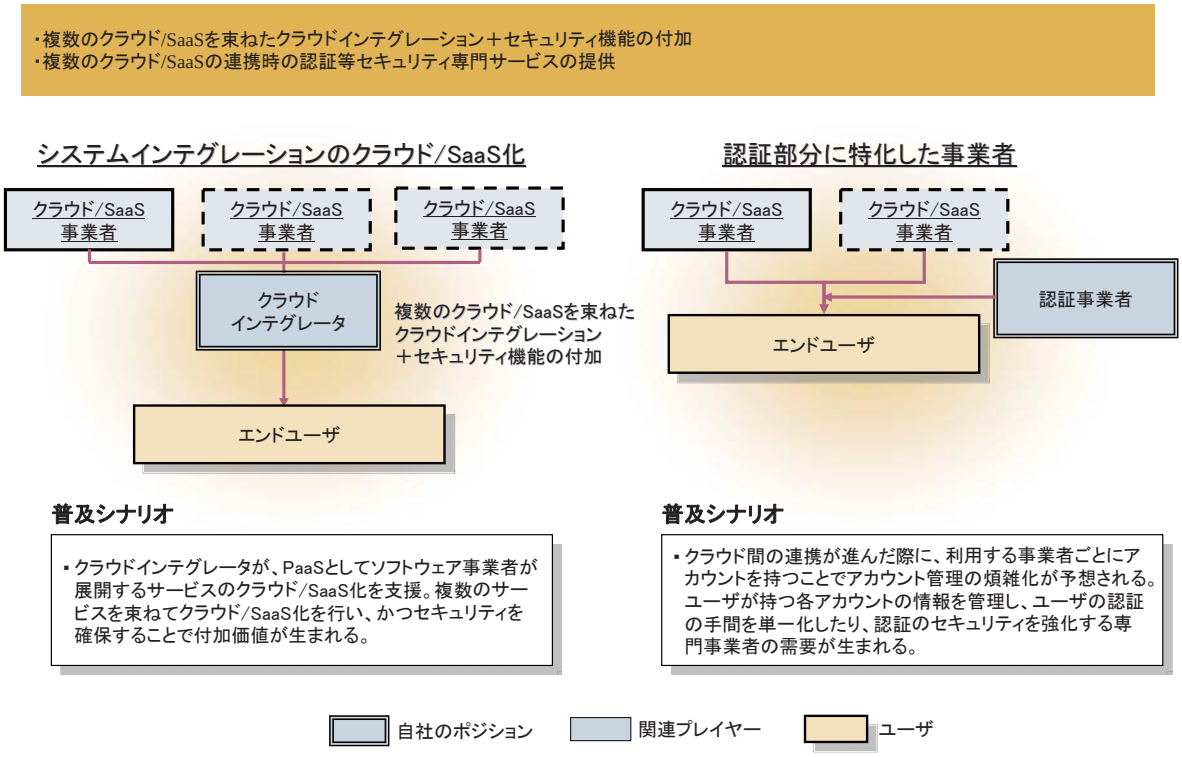


(2) 複数のクラウド/SaaS 事業者を束ねたクラウド・インテグレーション

ユーザのシステム利用形態が多様化するに伴い、複数のクラウド/SaaS 事業者を束ねたクラウド・インテグレーションが必要となる状況が生まれると、その対応は大手ベンダや SIer にしかできない領域であると言える。パブリック・クラウドとパブリック・クラウドのハイブリッド利用の場合の、全体システムの最適化と全体システムのセキュリティを確保するサービスの提供は最も有望なビジネスである。この際、ユーザ企業からはクラウド利用におけるリスクを吸収してくれる事業者に対する要望が強まることが想定されるため、クラウドを含めたシステムの一部の不具合や稼働不能に対する全体としてのリカバリを提供可能な事業者に強みが生じると考えられる。また、ユーザは自身のセキュリティレベルや最適なシステム構成を判断できないため、それらの評価が可能であることも強みとなる。

一方、事業者側としては、従来取引のないユーザに対して強みを見せることが新規開拓の鍵となるが、企業第三者的立場からのセキュリティ評価コンサルティングを契機とした改善サービスの提案も有望であろう。或いは、キラーアプリでアピールする、PaaS と既存システムの連携部分で勝負をするということも可能性としてあり得る。

図表 4-6　複数のクラウド/SaaS 事業者を束ねたクラウド・インテグレーション

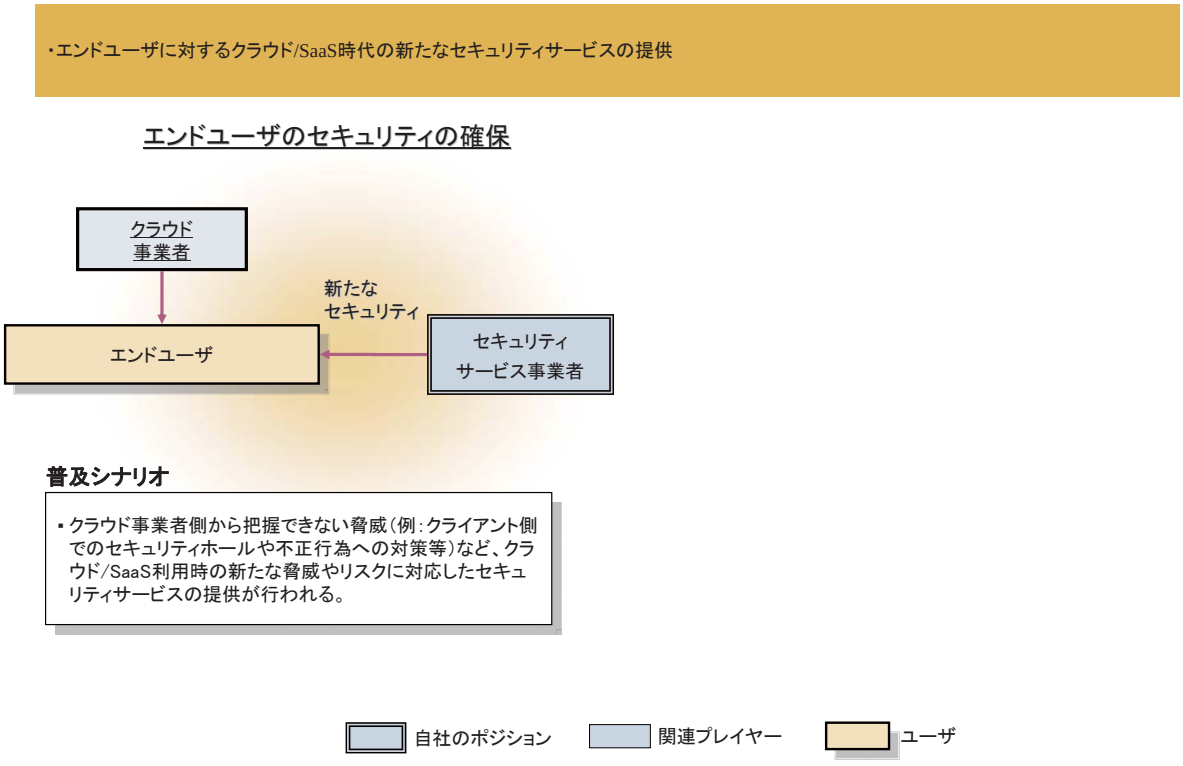


(3) エンドユーザに対する新たなセキュリティサービスの提供

クラウドの普及により、従来ユーザ企業が行ってきたセキュリティ対策の一部、或いは将来的には大部分がセキュリティサービスを取り込んだクラウド/SaaS 事業者によって提供される可能性がある。その場合、セキュリティサービス事業者にとっては、従来型のビジネスモデルを変革する必要が生じる。クラウド普及時代に、エンドユーザ側で行うべきセキュリティ対策が減少していくのか、新たなセキュリティ対策が必要となるのか、現時点では予測が難しいが、いずれにせよ、新たなセキュリティニーズへの対応、もしくは別の収益構造を検討する必要がある。

例えば、現時点ではクライアントレベルのセキュリティの需要は引き続き存在すると考えられるため、運用も含めたクライアントセキュリティサービスの提供は想定できる。但し、ユーザ企業の社内システムと連動しない部分であれば、ユーザにとっても事業者を乗り換えられやすいため、現状のクライアントセキュリティビジネスと同様シェアをどう確保するかが課題となる。クラウドにすることがビジネスではなく、シェアを奪われないようにすることを第一とし、クライアントを押さえることをベースとして、別のサービスに食い込んでいくビジネスモデルが有望と考えられる。

図表 4-7　エンドユーザに対する新たなセキュリティサービスの提供

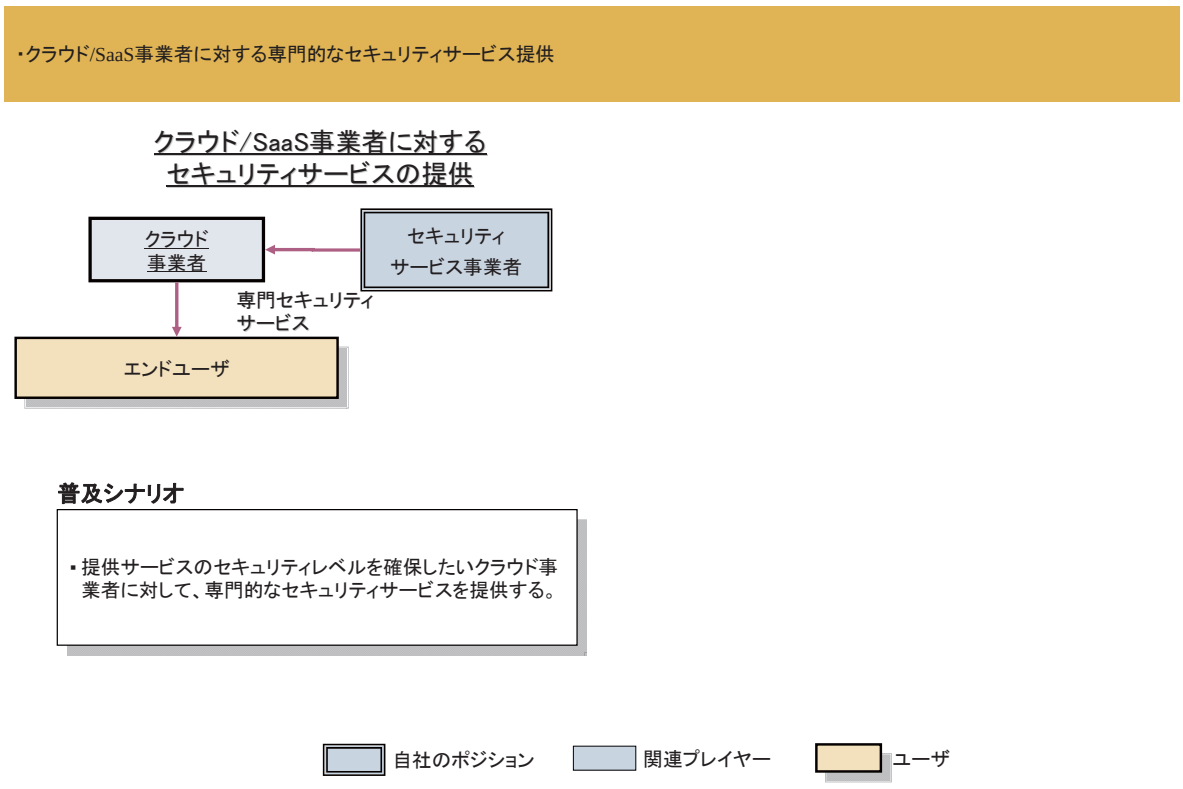


(4) クラウド/SaaS 事業者に対する専門セキュリティサービス

クラウド/SaaS の普及に伴い、クラウド/SaaS 事業者側にも高いセキュリティレベルを確保したサービスが求められる。この場合、クラウド/SaaS 事業者が自社で対応できないセキュリティ対策やセキュリティサービスについては、大手ベンダや SIer がクラウド/SaaS 事業者に対してセキュリティサービスやセキュリティを含めたインテグレーションを提供する形態も想定される。

現状、クラウド/SaaS 事業者はかなり大規模なセキュリティ投資を行っていることは確認できているが、それが自社のみで行っているのか、外部事業者を活用しているのかは明かされていない場合が多い。そのため、クラウド/SaaS 事業者側にどこまで外部活用のニーズがあるのか予測することは難しい。また、大手クラウド/SaaS 事業者は米国を拠点とするケースが多いため、日本の事業者にとってビジネスを展開することは必ずしも容易ではないと考えられる。とは言え、国内ユーザの高いセキュリティニーズに対応して洗練された高品質なセキュリティサービスは、海外のクラウド/SaaS 事業者にとって受け入れられる可能性はあるだろう。また、クラウド/SaaS 普及によって国内の中小規模のクラウド/SaaS 事業者が増加した場合も、セキュリティ対策について外部事業者に委託するニーズは存在すると考えられるため、そのようなクラウド/SaaS 事業者に対してセキュリティ基盤を提供するビジネスは想定されるだろう。

図表 4-8　クラウド/SaaS 事業者に対する専門セキュリティサービス



付　　録

付録Ⅰ　米国訪問調査結果（ヒアリングメモ）

ヒアリングメモ（Amazon Web Services）

October 14, 2009

Discussion with Steve Riley,

Sr. Technical Program Manager, Amazon Web Services (AWS)

Interview Notes

About customer concerns of moving to a cloud Architecture

“As companies consider using a public cloud they have to realize there is a difference between giving up control and giving up possession. By using a web service, we give up control of the infrastructure but not possession of the data. The same thing happens when we establish a VPN. We don’t control the traffic underlying a VPN but we maintain possession of our data with encryption.”

About service guarantees for security breaches

“Because security breaches frequently vary depending on what particular customers might be doing with AWS services, we don’t currently publish separate SLAs that cover attacks. Instead, we work with affected customers on an individual basis so that we can ensure the customer’s exposure is minimized. Remember, of course, that Amazon EC2 instances provide full root/administrator access. Therefore, instance and application security are primarily the responsibility of the customer: we do this to provide the customer maximum flexibility to choose their own security tools. Good security and management procedures will, more than anything else, reduce the likelihood and severity of attacks.”

About AWS physical security measures

“AWS is designed such that within each geographic region (US and Europe) there are multiple “availability zones”. These are physically distinct areas each with their own storage and computing.

The idea here is to spread the computing and storage across multiple physical locations. This reduces the likelihood that a fault at one location will affect the availability of the application.

We also have a lot of experience building large datacenters so we need how to keep them secure. We don't advertise that a data center is a datacenter. They are pretty non-descript buildings with very strong perimeter security. We use multi-factor authentication and only let people in that I have need to be there. In addition, all entries are logged."

About security and virtualization technologies

"We use virtualization technology to keep EC2 server instances separate from one other. We have worked closely with Xen and their Hypervisor product which have customized to our needs."

About encryption

"AWS does not encrypt any data. We prefer that customers choose what data needs to be encrypted and the method for doing that. Some customers use the file level encryption within that comes with Windows servers, other might use TrueCrypt for example which covers entire folders and volumes. "

About fending off hackers

"We have a group within AWS which focuses entirely on monitoring developments in the attack community. They are continually trying to improve our service to address any vulnerabilities that may arise."

About Amazon Security Certifications

"We continue to be compliant with SOX and have helped several customers successfully deploy HIPAA compliant applications. We are in the progress of becoming SAS 70 Type II certified and this will address our physical security, change management, and all of our web services."

About partners in the Security space

"With respect to our SAS 70 type II certification, when we publish the results of the certification, we'll also list the organizations we worked with to obtain the audit which include the audit firms and those involved penetration testing. enStratus is one of many ISVs we are working with to add value to AWS. But we do not recommend any one ISV over another; rather, we encourage our customers to

evaluate the full range of partner offerings and select those that best meet their business and technical requirements."

Thoughts on how the cloud computing era is affecting trends in the IT industry in terms of security or other.

"In general, cloud computing is changing traditional relationships. The cloud represents a broader trend of the consumerization of IT. Rather than companies buying (expensive) assets from vendors, consumers are purchasing on-demand services from providers. IT is transitioning to the notion of utility computing, which allows organizations to focus on their core businesses rather than spending so much time and money on undifferentiated activities that can more effectively be outsourced. The boxes and the software running on them really don't matter so much as do the protocols between them: your inventory protocol, your checkout protocol, your data retention protocol, your customer relationship protocol. These are where you derive maximum business value and competitive advantage. So let the cloud handle managing your boxes."

ヒアリングメモ（IBM）

October 20, 2009

Discussion with Kristin Lovejoy,

Director, IBM Corporate Security Strategy

IBM CloudBurst Project Office

Interview Notes

About what cloud computing and its impact on IT

“The conversation about cloud is really a discussion about new consumption and delivery models enabled by the new dynamic infrastructure that cloud computing represents. The term Cloud is used to describe a new relationship between those who use IT and those who consume it. Cloud enables users of IT services to focus on the services provided rather how than how they are implemented. From the end user perspective this means having the ability to log in from a self-service portal, select the resources required from a catalog, and have those resources provisioned immediately. From an IT perspective this means having a place to offer those resources and the ability to rent those resources to end users who can provision everything themselves. In other words, IT doesn’t need to spend time assembling and dissembling resources.”

About the need for Cloud computing security

“In spite of the documented benefits of the cloud computing model, adoption has been slow due to concerns about security. Security is usually the #1 concern for any new IT solution, but the additional ‘external’ aspects of the cloud exacerbate this concern. In specific, customers are concerned about having their data in public clouds. For example, they worry about ‘data persistence’. They wonder what will happen to their data once it is in the cloud because they have no control over how it will be handled. Most importantly even if they try to delete the data it can still persist in electronic form. However, large enterprises seem to be more interested in the concept of an Enterprise Cloud (aka private cloud), which they consider to be more secure than any external solutions.”

About the Cloud computing and SLAs

"Service Level Agreements must be managed such that the cloud vendor understands and adheres to a customer's unique business needs. We suggest that it addresses:

· Availability and uptime

· Who is managing the infrastructure? such as any third parties involved

· Data security. Particularly with respect to how the data will be handled by third parties or any third party partners.

· Vendor responsibilities- they should be clear and detailed (who is responsible for what)

· Vendor trust- and provisions for what happens if a vendor or third party goes out of business.

· Data migration and how it will be handled.

· Border & access constraints- in other words, what happens if the customer's data goes beyond local or national boundaries (some countries or states prohibit their data from leaving the region)."

About IBM's cloud security capabilities

"IBM approaches cloud computing in the same way it approaches all IT services- namely through the IBM Security Framework. The Framework presumes most organizations function similarly where you have people interacting with data, data residing on infrastructure, accessed through complex applications, over a network, to a physical facility. What IBM tries to do is understand what an organization's unique IT framework looks like and then we try to understand where the potential break-points are so that reasonable controls can be applied…However, security should not be a constraint but rather a value-add… IBM approaches security the way an automaker approaches building safety features into cars. Security has to be baked in and that's what IBM customers expect- so that is what we deliver with public and private cloud offerings. We see it as a must have and so we provide all the necessary best practice services and technologies to make the cloud secure."

About Cloud computing as a Security opportunity

"Cloud computing may seem complex but within it there is also an opportunity to simplify controls and defenses. Through cloud computing we are going back to a time of homogenous pools of resources. The homogeneous pools are much easier to manage from within the service management construct that lies at the foundation of cloud computing. In addition, data can now be managed centrally making it easier to secure, store and archive. So we shouldn't necessarily look at cloud computing as new and scary because the reality is that cloud computing presents some important opportunities as well."

About the Security of Public vs Private Clouds

"Customers tend to believe that Private clouds are better and more secure because they reside behind the firewall and the customer has full management control. But the reality is that a carefully customized security-focused SLA can actually be just as secure. A public cloud can also be more efficient and cheaper as the customer can negotiate pricing based on economies of scale. In other words, it all depends on the contract the customer has with the vendor and how well that contract adheres to the requirements of the customer."

About IBM's accountability with respect to data leaks

"This all depends on the contract. In general (and not specific to IBM), third party providers specify who is liable in the event of breach based on the SLA they have in place. So if a customer is concerned about this they need to make sure it's in the SLA. This is also not specific to cloud computing. Any time customer gives data to a third party, the SLA must address these issues."

ヒアリングメモ（Jericho Forum）

October 21, 2009

Discussion with Stephen Whitlock,

Chief Security Strategist, Boeing Corporation and Jericho Forum Board member

Interview Notes

About the work of the Jericho Forum

“The focus on cloud computing was initially formed as a year-long effort. I think it will probably be more than a year. I think the interest in how to protect data, no matter where it is, is what it really boils down to. IT systems exist to manipulate, share, and process data, and the reliance on perimeter security to protect the data hasn’t worked out, as we’ve tried to be more flexible.
We still don’t have good tools for data protection. The Jericho Forum did write a paper on the need for standards for enterprise information protection and control that would be similar to an intelligent version of rights management, for example. ”

About recent Security measures from the Jericho Forum

“A lot of discussions around cloud computing get confusing, because cloud computing appears to be encompassing any service over the Internet. The Jericho Forum has developed
what they call a Cloud Cube Model that looks at different axis or properties within cloud computing, issues with interoperability, where is the data, where is the service, and how is the service structured. They've also coupled that with the layered model that looks at hierarchical layer of cloud services, starting at the bottom with files services and moving up through development services, and then full applications.

The combination of the axis -- and it gets problematic to represent more than three or four dimensions on paper -- may determine the viability of a specific cloud service. For example, if your organization has no skill in building a cloud service, but want to do it internally, then you
may outsource the development to a cloud service provider that’s skilled at building those services. If you don’t want internal infrastructure and want to leverage the agility of the cloud service, then

you may find yourself in the external and outsourced services of leveraging one of the common commercial providers.

In addition to the cube model, there is the layered model, and some layers are easier to outsource. For example, if it's storage, you can just encrypt it and not rely on any external security. But, if it's application development, you obviously can't encrypt it because you have to
be able to run code in the cloud. I think you have to look at the parts of your business that are sensitive to needs for encryption or export protection and other areas, and see which can fit in there. So, personally identifiable
information (PII) data might be an area that's difficult to move in at the higher application level into the cloud."

About how Cloud computing is affecting IT

"(Cloud computing has) grown very fast. A part of me has been surprised, but I also see a relabeling of existing services as cloud services -- SOA and other services. The growth doesn't surprise me too much, given the flexibility. I am worried about the accompanying risks. Cloud is a broader concept…There is still a lot of hype in this area. I believe there is something there that may not resemble all of the hype and the press we've seen about it. Similar to SOA, the idea of direct interactive services on demand is a powerful concept. I think the cloud extends it. If you look at some of these other layers, it extends it in ways where I think services could be delivered better.

It's also very important to be able to withdraw from a loud service, if they shut down for some reason. If your business is relying them for day-to-day operations, you need to be able to move to a similar service. This means you need standards on the high level interfaces into these
services. With that said, I think the economics will cause many organizations to move to clouds without looking at that carefully."

付録 II　講演録

講演録（Salesforce.com）

日時	2009 年 8 月 26 日（水）16：15－17：05
場所	(財)日本教育会館 9 階 902 会議室
講演タイトル	「セールスフォース・ドットコムの情報セキュリティ対策の取り組み」
講演者	株式会社セールスフォース･ドットコム シニアプリンシパルアーキテクト 内田 仁史 氏

講演概要

Salesforce.com 社（以下 Salesforce）が実施している情報セキュリティ対策について、同社が持つシステムインフラ、サービス提供の状況・セキュリティ投資等のバックグラウンドをご説明いただいた上で、機密性・保全性・可用性に監査性を加えた 4 つの観点から具体的対策をご紹介いただいた。

講演の要点

1　Salesforce の情報セキュリティ対策のバックグラウンド

- Salesforce では、一般的に言われる情報セキュリティの CIA、つまり機密性・保全性・可用性に加えて、監査性を含めた 4 つの観点において、大規模なセキュリティ投資の下、広範囲なセキュリティ対策を行っている。
- Salesforce の提供サービスは B to B を対象としているため、他のクラウド/SaaS 事業者に比べデータセンターのシステム規模としては大きくない。西海岸にメインセンター及びラボ&テープバックアップセンター、東海岸にディザスタリカバリ用のサイトを所有しており、さらに今年日本を除くアジアパシフィック向けセンターをシンガポールに設置している。メインは西海岸とシンガポールのサイトであり、サーバの数としては 1,000 台強である。センターでは 2005 年に 60 億円以上を投じてシステムを一新しており、さらに毎年数十億円規模のセキュリティ投資を行っている。
- 一般的にセキュリティは、「何も起こらないこと」への投資であり、その必要性について経営陣から理解を得るのは難しく、また実際にリスクも踏まえて幾ら投資すればいいのかを考えても、一般企業におけるセキュリティ投資には限界がある。一方、Salesforce の場合、システムインフラを一極集中化させており、そこで扱うデータは、企業のリアルタイムな商談情報など非常にセンシティブなものである。情報セキュリティレベルは投資費用に比例するため、こういった環境に対して、集中的に大規模な投資をすることで、1 社では出来ないセキュリティ対策を実現している。
- Salesforce のサービスの場合、ユーザ単位で徴収する利用料金の一定の割合をセキュリティ投資に当てているため、確実なセキュリティ投資が可能となっており、また規

模の経済によってセキュリティのレベルも向上している。

2　機密性に関する取り組み

2.1 物理的セキュリティ

- Salesforce の各データセンターは自社所有ではなくファシリティとして借りているものだが、システムの運用に関してはアウトソーシングを一切行っていない。また、Salesforce が借りている区画に入るためには 5 段階のバイオメトリクスの認証があり、データセンターの管理会社の人間も Salesforce の許可がなければ入ることが出来ない仕組みとなっている。さらに、社内の人間でも出入りできる人間は制限されており、彼らもマネージャの申請を経て、許可された時間内のみ入室が可能となる。

2.2 ネットワークセキュリティ

- セキュリティホールに対しては、CERT/CC 等あらゆる情報ソースから常時情報を収集しており、契約する複数のセキュリティベンダ、専門コンサルタントとも連携して、パッチ適用等の対策を実施している。また、システムはオープン系の Linux がメインでマイクロソフト社の製品は一切使っていない。
- 組織的には 24 時間 365 日監視/運用体制をとっている。また運用体制からは完全に独立したセキュリティ専門組織が設置されており、セキュリティスペシャリストを揃えている。さらに、各セキュリティベンダが提供する最高位レベルのサービスの契約を結び、セキュリティコンサルタントとも契約をしている。
- 脆弱性評価に関しては、複数の第三者機関による継続的な評価を受けており、ネットワークに関しては 4 ヶ月に 1 回、アプリケーションコード（SQL、クロスサイトスクリプティング）に関してはバージョンアップ毎にチェックを受けている。チェック方法は、各プロバイダのノウハウであり、なるべく多くの評価を受けることで評価精度が上がると考えている。また、少数ではあるがお客様から独自に評価をしたいという要望もあり、実際に幾つかのテストを実施しているが、どのケースも全く問題ないという結果であった。
- また、経済産業省で採用されたエコポイントのシステムは、バックオフィスに使うもので、初めてパブリックサイト上にロジックを組んでいるが、脆弱性に関しては全く問題ない。

2.3 インターネットセキュリティ

- インターネットのセキュリティに関しては、現状で 128 Bit の SSL の暗号化が破られることは考えにくく、十分なセキュリティが確保されていると考えている。例えば、VPN を採用すればプロバイダとしてはセキュリティを担保しやすく、お客様の安心感も得られるが、セールスフォースでは敢えて利便性を重視してインターネットから直接アクセスできる形にしており、一方で紹介したような強固なセキュリティ対策を敷くことで安全性を担保するという姿勢をとっている。
- 但し、日本のお客様に対しては NTT コミュニケーションズと連携して VPN サービス

を提供している。月々の料金としては上がることにはなり、セキュリティレベルに違いはないが、心理的な安心感と経営層を説得しやすいという理由で選択されるお客様が多い。

2.4 内部漏洩対策

- データはすべてデータセンターに格納しているが、お客様のデータはお客様の所有となるため、Salesforce 側では一切触ることが出来ない仕組みとなっている。Salesforce 側がアクセスできるのはデータベースだけで、その権限を持つのも米国本社の少数の人間のみである。データ自体にはアクセスできない上、マルチテナントの形式をとっており、データベースをそのまま見ただけでは情報の利用価値はない。データベース管理者の操作に関しては、相互検証体制という形ですべてがモニタリングされており、発行されるコマンド、スクリプトに関してはすべて事前承認が必要となっている。発行したコマンドに関しては、別の管理者を置いた集中化されたログ管理システムにリアルタイムにコピーされるため、改ざんは不可能となっている。また、システム運用部門はすべて正規社員のみであり、当然すべての社員に対してかなり厳しいバックグラウンドチェックを行っている。

2.5 集中化されたセキュリティコントロール

- 集中化のリスクについてもお客様から指摘を受けることは多い。確かに日本のマルチテナントのデータがハッキングされた場合、他のお客様のデータも漏洩してしまうのは事実だが、この場合のリスクは Salesforce 自体の最大のリスクであり、だからこそこれまで紹介したように、優秀な人間に高いサラリーを払って管理を徹底している。
- マルチテナントでの集中化の規模についても、現時点で Salesforce 程の規模を持つ事業者は他にない。管理するサーバ類の量やレベルも増えてくると、管理者の非常に高度なレベルが求められるのが当然であり、それに合わせて日々人員も増強している。

2.6 利用ユーザに対するセキュリティ

- 利用ユーザに対するセキュリティに関しては、Salesforce のアプリケーションサービスとして、データアクセス権限、ユーザ権限の詳細な設定など、企業の要望に応じた様々なオプションを用意している。
- また特徴的なサービスとして、ログイン IP アドレスの制限も行っている。例えば、ログインできる IP アドレスを社内のグローバルアドレスに限定することで、外部からはログインできないシステムを実現することが出来る。また、VPN のリモートアクセスインフラを持つ企業については、そのインフラをそのまま利用できるため、社内と同等のセキュリティを担保することが出来る。
- 一方、IP アドレスの制限を行わずに、ID とパスワードが盗まれた場合にも、信頼できる IP アドレスを予め登録しておけば、それ以外の IP アドレスの場合は初回のログインに際し、メールで本人確認のステップが必要となり、以後は過去にログインした IP アドレス及び PC であればメール確認抜きでアクセスできるようになっている。

3　保全性に関する取り組み

- データセンターでは disk to disk のコピーを行うシステムを持っており、データセンター間ではリアルタイムのレプリケーションを行っている。ラボにあるアーカイブセンターでは 24 時間毎にテープバックアップも行っているため、データがデータセンターの外に出ることは一切無い。またお客様自体のバックアップオプションもサービスとして用意している。

4　可用性に関する取り組み

- ネットワークに関しては、設立当初は米国系のキャリアのみだったが、ここ 2～3 年は米国に乗り入れている日本のキャリア 4 社のうち 3 社とトランジット及びピアリングという形で契約しており、それぞれのキャリアを使っているユーザは、単一のネットワークで接続できるため、ISP 間の接続部分でのトラブルは大幅に減り、パフォーマンスも向上した。
- 集中化されていることでパフォーマンスが落ちることを懸念するお客様もいるが、日々増加するトランザクション（日々約 2 億件）に対して、平均のサーバのページ処理時間は減り続けている。これは、アーキテクチャが水平・垂直のスケーラビリティを持ち、日々メンテナンスをしてシステム拡張を行っていることによる。
- また、物理セキュリティの部分で紹介したように、データセンターに関してはワールドクラスのセキュリティが確保されている。

5　監査性に関する取り組み

- システムについては、誰でもアクセスできる“trust.salesforce.com”というサイトにシステム稼働状況を公開しており、各エリアのインスタンス毎にシステム状況、処理トランザクション数、平均レスポンスを表示している。
- また日本独自の取り組みとして(財)マルチメディア振興センターの「ASP・SaaS 安全・信頼性に係わる情報開示認定制度」における認定の第 1 号を取得している。この認定取得に際しては審査対象項目に対して回答するだけではなく、実際のエビデンス情報も提出した上で審査を受けているため、信頼性は高いと言える。
- お客様からの定期的な委託先監査としては、SA70 Type II に基づく監査を受けている。個人情報保護の場合、アンケートやヒアリングの形式で確認を行うことが多いが、ベンダ側の回答の信頼性は担保できない。一方で、お客様の契約した監査人が事業者のデータセンターすべてを監査するのも現実的ではない。その中間として SA70 Type II に基づく監査が適していると考えている。Salesforce では独立系の監査法人より、サービス提供に関する内部統制及びセキュリティに関して継続的な監査を受けている。この監査レポートをお客様に提供し、それをお客様自身が確認することで、間接的に監査を実現している。SA70 Type II は 1 年の監査期間で費用もかかるものだが、Salesforce では 2 つの監査プロジェクトを 6 ヶ月毎に回しているので、6 ヶ月毎に監査

レポートを出すことが出来る。また、お客様から求められるチェックシート、アンケート、訪問調査なども随時受けている。

- こうした実績を示すことで、多くのお客様の信頼を受けており、大企業やセキュリティビジネスを行う企業、さらには米国政府機関等、セキュリティに厳しい組織からも採用されている。
- お客様がこれらと同等のセキュリティを確保しようとすると非常にコストがかかる。クラウド/SaaS だからこそ規模の経済を利用してこのようなセキュリティレベルを実現することが出来ると考えている。

以上

講演録（経済産業省）

日時	2009 年 8 月 26 日（水）15:00 – 16:00
場所	(財) 日本教育会館 9 階 902 会議室
講演タイトル	「クラウド・コンピューティングに関するセキュリティ関連政策の動向」
講演者	経済産業省商務情報政策局情報セキュリティ政策室 課長補佐　清水 友晴 氏

講演概要

基礎的な知識として、クラウド・コンピューティング技術及び、それら技術に基づいたクラウドサービスにおいて現在顕在化している技術面、制度面、運用面におけるセキュリティ上の懸念事項についてご説明いただき、それらへの解決策として経済産業省が推進するクラウド・コンピューティングに関するセキュリティ関連政策に関してご紹介いただいた。

講演の要点

1　クラウド・コンピューティングについて

- クラウド・コンピューティングはハードウェアの抽象化・仮想化とサービス提供の 2 つのレイヤによって構成されており、これらを組み合わせることによって、柔軟な構成を実現できることが大きな特徴である。
- クラウドサービスの特徴として抽象性と弾力性がある。ユーザはクラウドの中身は見えないが、クラウド中に存在している機器を必要に応じて抽象化された計算機リソースとして提供される。また Amazon や Google のクラウドサービスに代表されるように、クラウド内のドメイン間でリソースを融通できるため、高い弾力性を持つ。特に Amazon では Amazon 自体で多数の計算機を持っているが、これらはピーク時を想定したものであるため、通常空いている部分をユーザに対して提供することが出来る。これまでもオンデマンド・コンピューティング、ユーティリティコンピューティング等の考えもあったが、クラウド・コンピューティングでは必要なときに必要な計算機リソースを従量課金で利用できるため、自社リソースと上手く組み合わせることで、リソースの最適化が出来る。
- クラウドの形態には HaaS/IaaS/PaaS/SaaS という分類がされている。HaaS ではユーザに対して仮想的な計算機が提供され、ユーザ自身が OS やアプリケーションの導入を行うため、既存のアプリケーションをそのまま動作できる利点がある。IaaS では、仮想インスタンスまで提供され、ユーザは自分のアプリケーションを導入して利用する。Google App Engine や Salesforce.com 等に代表される PaaS ではユーザにプログラム実行環境までが提供されており、ユーザ側でアプリケーションを管理できるため、カスタマイズにも向いている。日本の場合、受託開発で自社に合わせて開発してきたシステムが

多くあり、こうしたシステムを活用するためにも PaaS は有効と考えられる。SaaS はクラウド上で動作するアプリケーションに Web ブラウザをユーザインタフェースとしてアクセスする形式である。アプリケーションを持っていないユーザにとっては、コストも安価であり利点もあるが、逆に既にソフトウェア資産を持っている企業にとってのメリットは少ないと言える。経済産業省でも中小企業向けの J-SaaS のサービスを開始しているが、実際には予想したほどにはユーザ数が増えていないと聞いている。

2　クラウドに対する問題意識

2.1 国内 IT 企業の国際競争力維持・強化

- Google や Amazon などの海外企業が先行しており、国内 IT 企業、特に大手ベンダのクラウド開発・展開を促進する必要がある。
- 総務省では霞が関クラウド、自治体クラウドなどの取り組みが進められている。自治体クラウドに関しては全国から複数の自治体でそれぞれ5億円規模の実験が行われており、自治体の情報処理システムをクラウドで展開することを目指している。これまでにも共同利用 ASP の取り組みもあったが、業務の標準化が進んでいない自治体では利用が難しかった。今回は、近隣の自治体間での共同利用という形なので、全体としては情報システムの効率化が可能だと考えている。

2.2 国内企業の IT 利活用推進

- 受託開発中心の IT システム環境では、SaaS としてのクラウド利用は進まないため、我が国の特殊な IT 利用事情に対応したクラウド構築を推進する必要があると考えている。大手事業者へのヒアリングでも同様の意見が得られており、現状受託開発のシステムを持つ企業でもクラウドを利用していくために、既存のハウジングやホスティング環境をクラウド基盤に利用することで安価にクラウドを実現するためのモデルを考えなければならない。
- データを共有システムに預託することに対する不安が高いことから安全性を担保する技術開発を支援する必要があり、これに関する研究開発は後で説明する H21 年度の事業の中で進めている。

3　クラウドに対するセキュリティ上の懸念

3.1 技術面

- 仮想化技術に関してはクラウド環境で用いられている仮想化技術自体にも脆弱性が発見されており、また未知の脆弱性が存在する可能性も否定できない。
- クラウドは一種の共有システムであることから、データの機密性確保のために暗号処理を施すべきだが、クラウド事業者が暗号鍵を保有管理しては内部犯行対策にならない。
- 複数のクラウド事業者を利用し、クラウド毎に認証が必要な場合、情報漏洩や既存のリスク、アカウント管理のコストは増大するが、1 つのクラウドにおける情報漏洩が他のクラウドに影響することはない。一方、OpenID 等クラウド間で認証連携を行っ

た場合、ユーザの利便性は向上するが、ユーザ登録したクラウドで情報漏洩が起こると、他のクラウドに悪影響を与える可能性がある。幾つかのクラウド事業者間では連携が行われている例もあるが、さらに認証認可に特化した高セキュアな ID プロバイダの必要性も考えられ、実際には Liberty Alliance でも同様の検討が行われていると聞いている。

3.2 制度面

- コンプライアンスに関して、何か事件があった際にサービス事業者がデータ開示を法的に求められた場合、ユーザから拒否を求めることは出来るかという点について、現時点では事例がないが今後検討が必要あると考えている。
- データが国境を越えて流れる場合、どの国の制約を受けるのかについては非常に大きな課題である。現状では大手クラウド事業者のデータセンターは各国に散らばっており、自社のデータがどこにあるかを特定することは難しい。欧州に関しては、EU 域外には出さない、出すのであれば許可が必要という規制が行われている。
- クラウドのような IT アウトソーシングも内部統制の対象となっており、SAS 70 Type II 報告書などの提示をクラウド事業者に求める必要がある。通常この種の報告書はクラウド施設全体に対して作成するものであるが、外部のサービス事業者を自社の内部統制の範疇に含めるかどうかは企業によって異なり、そもそも非上場企業等、内部統制報告書提出義務のない企業も多いことから、内部統制対応の費用負担についての考え方について基準が必要である。
- 監査については、特定のユーザの使用（予定）範囲を特定する必要があるが、フレキシビリティがあるクラウドでは、その特定は難しい。また監査の中で求められるシステムの詳細の開示については、広大なデータセンターを有するクラウド事業者等の場合は現実的ではない。本年度の実証実験では、クラウド事業者が外部監査人と契約して外部監査を受け、ユーザに対してはその報告書の概要を示すというモデルについて検証している。但し、この監査人はユーザが契約した監査人ではないため、どこまで信頼性があるのかは検討が必要である。他にもどういったモデルが考えられるかについて、本年度の事業の中で日本セキュリティ監査協会（JASA）とも相談の上協議していく。

3.3 運用面

- クラウド事業者のサービス終了や倒産に際して、契約条項でサービス停止についての事前予告を定めたとしても、その契約上の義務が必ず守られるとは限らない。
- 稼働しているシステム、しかも複数組織の大量のユーザがオンラインの状態で脆弱性対策のパッチ適用などが出来るかについては、複数のユーザがいる場合、個別に許可をとることはできないため、事業者側で一方的にサービスを止める可能性もあり、SLA でも保障できない部分があると考えられる。クラウドの場合、どうしても個々のユーザへの対応が出来ないという面があるため、今後プライベート・クラウドやパブリック・クラウドとプライベート・クラウドのハイブリット・クラウド等、クラウドの多様化が進むと考えている。

4　クラウドセキュリティに関する政策

・ クラウドセキュリティに関する政策としては、H21 年度の補正事業として「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」を実施する。具体的には以下の 4 つの検討を行う。

【クラウド環境におけるセキュリティ検討会開催】

・ 3 において紹介した技術的課題、制度的課題、運用的課題についてまとめる。

【クラウド環境に適した次世代セキュアプラットフォームの検討】

・ 現状、デスクトップ OS やサーバ等、大部分のプラットフォームが海外の企業に寡占されている状況にあるが、クラウドへのパラダイムシフトを機に、今後の IT 環境のあるべき姿を議論しまとめる。

【クラウド環境活用に向けた企業内既存システムとの連携実証実験】

・ 認証認可に関する実証実験を行う予定であり、クラウドサービスのアカウントを社内のアカウント管理システムと連携させることで、簡単、安価でかつ、クラウド事業者にアカウント情報を預けないでクラウドを利用するための技法について研究開発を行う。

【クラウド環境における効果的なセキュリティ監査技法の検討】

・ 3.3 でも紹介した外部監査について、①クラウド事業者が、外部監査を実施、結果を開示するモデル、②クラウドユーザが利用範囲に関する外部監査を実施するモデルの 2 つのモデルの検討を考えているが、実際にはパブリック・クラウドにおいて利用範囲特定するのは難しいため、②はプライベート・クラウドやそれに準ずる環境での適用になるだろう。

・ H22 年度では洗い出された課題への対応、必要な研究開発を行う予定である。セキュアプラットフォームに関しては 3〜4 年の期間が必要だと考えており、最終的には実際にプラットフォームを開発するところまでを目指したいと考えている。

5　アウトカム・アウトプットのイメージ

・ 国内サービス事業者のクラウド対応について、Google、Amazon、Salesforce.com といったグローバル展開を進めるサービス事業者に対抗できる技術力、経験の蓄積を後押しし、さらにはクラウド・コンピューティングのグローバルリーダーとなり、顧客を国外に求めていくことが出来るように継続的に推進していく。

・ 国内ユーザ組織のクラウド対応促進として、組織ユーザの懸念であるデータ保護を確実に提供する技術的な保証、サービス事業者のセキュリティ対策を第三者監査により確認、既存 IT システムとクラウド環境の統合シナリオ作成等を考えている。

以上

講演録（札幌市 SaaS ビジネス研究会）

日時	2009 年 10 月 1 日(木)13：30－16：30
場所	札幌市エレクトロニクスセンター
講演タイトル	「札幌市 SaaS ビジネス研究会の活動のご紹介」 「会員企業様によるビジネス取り組み内容のご紹介」 ・人材開発株式会社 ・株式会社つうけんアドバンスシステムズ
講演者	財団法人さっぽろ産業振興財団　情報産業振興部情報産業振興部長 松田 祐至　氏 財団法人さっぽろ産業振興財団　主任研究員　山下 幸修　氏 人材開発株式会社　代表取締役社長　伊藤 直樹　氏 株式会社つうけんアドバンスシステムズ エンタープライズソリューション事業部　担当部長　中島 弘幸　氏

講演概要

札幌市 SaaS ビジネス研究会の活動についてご紹介いただき、SaaS 展開事例等の説明をいただいた。また、研究会に属する人材開発株式会社、株式会社つうけんアドバンスシステムズの 2 社から、ビジネス取り組みの現状とセキュリティ対策の考え方、ユーザニーズ、今後のクラウド/SaaS の普及予測等についてご講演いただき、委員会委員との意見交換を行った。

講演の要点

1　札幌市 SaaS ビジネス研究会の活動のご紹介

<< 講演 >>

- 研究会には 60 社程度が参加。パートナー企業として、マイクロソフト、富士通、NTTPC コミュニケーションズ、日本電気等に協力いただいている。
- 主要な活動は、パートナー企業のセミナー、ビジネス活動（タスクフォース）・人材育成、他の研究会やイベントへの参加、ビジネスデベロップメントセッション（BDS）等。
- セミナーはパートナー企業以外にも協力。ASP・SaaS インダストリ・コンソーシアム（ASPIC）の協力を得て共同セミナー等を実施している。研究会参加企業の幾つかは全国 SaaS ベンダ連合会にも参加。
- ビジネスデベロップメントセッション（BDS）は、マイクロソフトが 2 ヶ月程度で研修を行い、実際にビジネス展開を開始。
- 主なビジネス活動は以下の通り。
  - 医院/クリニック向けレセプトオンライン請求サービス：レセプトオンライン請

求義務化への対応、研究会から 2 名が参加。

- 公的機関の申請手続き：SaaS を展開する前段階として、SaaS ビジネスのインキュベーションとして活用を促進。
- 公立学校（小・中・高）向けのサービス（事務、教務）：ビジネスデベロップメントセッションからサービスへ展開。
- 大学教職員等の安否確認サービス
- 一般流通向けのサービス
- 弁護士向けのサービス

・ 霞が関クラウドが石狩に建設予定。連携して推進していきたい。

<< 質疑応答 >>

・ レセプトオンライン義務化、予算はどのような形でとっているか。（吉田）
  - 詳細はまだ決まっていない。推進側と本業重視派と 2 通りいる。法律で決まっており、いずれやらなければならないが、これからという状況。（山下氏）
  - 対応できない高齢の開業医が廃業しなければいけないという問題も北海道の新聞に採り上げられた。（松田氏）
  - 拒否反応を示す医者がいるのも事実。（山下氏）
  - 代行サービスを行う医師会もいると聞く。サービス展開の仕組みの中で検討してもよいかもしれない。（遠藤委員長）
・ 公共ポータルのプラットフォームは自前か、パブリック・クラウドなのか。（遠藤委員長）
  - 独自プラットフォームを予定している。（中島氏）
・ 経済産業省の講演では SaaS の普及が進まない、既存ソフトウェアベンダが SaaS を展開したがらないという現状があるとのことだが、札幌の状況はどうか。（遠藤委員長）
  - 概ね同じではないか。札幌の IT 企業の事業構造の問題もあるが、要件定義を受けて、売り切るという形が多かった。この時代、ユーザ側で設備投資ができない場合、作るより利用に回らざるを得ないという意識を持ち始めている企業もいる。システムを作ってもすぐにお金にならないところも問題。何をきっかけに進んでいくか。どれだけキラーコンテンツ、サービスを提供できるか。研究会としてきっかけが作れると理想だが、具体的に何かはまだ議論できていないところ。（山下氏）
  - 時代の流れはクラウド/SaaS に行くのはわかるが、真っ先に行く所と人が動いた方が早いという企業が 2 通り。そうこうしているうちに、海外企業に浸食されてしまうというという周知が必要。
・ クラウド/SaaS は地理的にも札幌の IT 企業にとってビジネスチャンスと捉えられているか。（江連）
  - クラウド/SaaS は、札幌の IT 企業にとってビジネス拡大のチャンスだと思うが、

商材になりそうなところがあれば紹介するという形を行っている。市の事業所等へのお声かけは行っている。儲かるか儲からないか、規模の問題もあり、民民の連携が重要であると認識している。東京圏の企業とビジネスマッチング的なところ､商材を組み合わせて SaaS に見せる等はできる｡コミュニケーション、お客さんを知ることが必要なので、マーケットを大きくする手段としてはあるが、実際に進める中ではどう売るか、どう営業するかも重要。そういう場を提供することが役割であると考えている。提供の形態がたまたま SaaS だったという流れが自然。（山下氏）

- 研究会企業は SaaS をまだ検討している企業の方が多い。（山下氏）

・ 弁護士向けのサービスはどのようなものか。（吉田）

- まだ検討中という段階。連合体があるところがサービスを展開しやすい。教育機関も同様。幾ばくかの動きはある。（山下氏）

・ この研究会では、ビジネス展開のしかけを作るのか。（平木）

- 頼るところが出てきてしまうので、すべてをやる訳ではない。企業が集まってやる部分を大事にしたいが､それだけでは動かないので､しかけも作っている。（山下氏）

・ パートナー企業のセミナーで言われるようなクラウド/SaaS のビジネスチャンスと、これから SaaS を展開しようとしている企業の意識にギャップがあるように感じる。現実感として、手応えはどうか。（川口）

- 個人的には、手応え的にはまだまだ。SaaS に近い形態は既に展開しており、何ら新しいものではない。クラウド/SaaS という言い方で逆にハードルが高くなっている面もあるのでは。延長でもあるが、新しいからやる、という企業もあるが、やろうとしていることに、大きな違いはないのではないか。所有より利用の形態に移る中で、上手い移行ができれば、普及していくのではないか。（山下氏）
- 本研究会では、シニアアドバイザーとして赤羽氏という IT 業界に長年携わっている方がいるが、赤羽氏はクラウドにとても熱くなっている。専門の方が情熱を持っている。データセンターが持てるような機構。データセンターがあるから、クラウド/SaaS 化が進む。札幌として力を入れていくべきではないかと感じる。（松田氏）

・ 中小企業が上手く活用できる仕組みを考えているか。（平木）

- 仕組みは作れると思うが、使いたいと思うソフトウェアがあるかどうかが重要ではないか。（松田氏）
- やれるところは既にやっているのではないか。データセンターが役立つのは、どれだけのデータが来るかどうか。霞が関クラウドなども動きもある。北海道にあることで、場所・環境だけでなく、それに絡めて新しいビジネスが拡大できるような土壌があるのが札幌ということを考えていきたい。既存のサービス

だけでは発展はない。（山下氏）

2　人材開発株式会社様によるビジネス取り組み内容のご紹介

<< 講演 >>

- SaaS については、モニタの意見を聞きながらシステム改修を含めているところ。
- 札幌の立地を踏まえると、なかなか上に上がるのが難しい。
- 大手企業では、自社ソリューション的な発想があり、SaaS は簡単には進まないだろう。中小は社会的認知が進まないと難しい。
- 函館事業所で介護事業を行っている。介護事業で利益が出ていたので、ベンチャー的にできるのではないかと思った。SaaS が普及してからでは遅く、売れなくても自社で使えるだろうということで始めた。
- 介護事業の請求システムを考えている。メインでやっていきたいと考えているが、マーケットとしては中小・零細なので、SaaS で使えるのは中小・零細ではないかと考えていた。介護事業は労働集約的。職員の ICT に関するナレッジもあまり高くない。函館にシステム管理者も置いていない。
- 介護事業者は早期から電子請求を要求されていた。零細であろうと、大手であろうと一括管理。業務上非常に大変。しかもサーバを置かなければならない。システム周りの人間を置く訳にもいかない。介護事業で純粋に利益率を上げる、利益効率を高めるために、SaaS を使えば自社内では少なくとも上手くいくだろうと思った。
- 情報セキュリティ対策は、函館では、クライアント PC レベル（Symantec）で管理、サーバは VPN で管理。現実問題として、パッケージソフトは初期費用がとても高い。一事業者で 100 万単位。年間運用コストも 30 万。固定費用が上がって大きな売り上げがない事業者は黒字転換できない。PC に詳しい人間を内部に置かなければならず、なおさら利益が上がりにくい構造になっている。
- SaaS を使えば、人を置かずに提供側で改善していけばよいものができるのではないか。失敗しても自社で利用できればよい。
- 文書管理システムとストレージ機能を組み合わせた SaaS アプリを提供している。開発のための基礎資料を作成するために。介護事業の利益だけで開発は難しかったので、北海道からの補助金を基に開発を行った。
- 一番のネックはデータセンターだった。コンサルタントやプラットフォームベンダのプレゼンを受けたが、初期費用があまりにも高い。試験的に運用しようと思っていたのに、その固定費用をどうやって取ればよいのかわからず、何から何まで自分でやらなければならなくなった。結局、どこの支援も受けずに自社だけでやった。マネジメント、技術系、人を集めて大変な思いをした。
- もともと ISMS を受けていたので、サービスを提供するのにあたり、その経験を踏まえ、規格要求を組立てていった。ISMS を持っていて、自社の取り組みのスコープの中でデータセンターを使える環境でなければ、実現は難しかっただろう。

<< 質疑応答 >>

- 開発期間はどの程度かかったか。（江連）
  - 補助金を受けるときには半年で申請していたが、きっちり 1 年間かかった。完全に機能が埋め切れていない。SaaS は機能を埋めていけるので、7 割方できている中で使っていただき、実装を進めて運用しながらノウハウを蓄積し、試行錯誤しながらやっている。これなら売れるという時点で、広告費用をうっていこうと思っている。（伊藤氏）
- ハードウェアは自前か。（平木）
  - サーバ自体はレンタルである。組立てるノウハウは持っているが、リスクアセスメントをすると、故障・不具合があった場合に困るのでレンタルにした。基本的にその他もレンタル。
- 開発時に苦労した点はどこか。（江連）
  - マネジメントの点が大きい。開発自体は Web アプリを作っていた会社なので、SaaS に展開するのはそれほど困難ではなかった。しかし、電算センターの使用、契約の問題、売上フローを描ききれない等の課題はあった。また、マンパワーにも限りがあり、開発中の売り上げがなく、開発余力も奪われていく。スピードではなく、協力会社の力を借りず、自社内のマンパワーでどこまでやれるか。（伊藤氏）
- 認証等の仕組みはどのようになっているか。（遠藤委員長）
  - ID、パスワードを利用。ユーザは士業なので、セキュリティの問題は大きい。第 2 弾の開発としては、USB トークンを使う予定。現在はワンタイムパスワードを使っている。モニタに対して一部カードを使っている。試験的に実施している。売れるものを開発しなければならず、機密性と可用性はバランスの問題なので、どこまでをやるかはこれからの検討課題である。（伊藤氏）
- エンドユーザからのセキュリティに関する要望はあるか。（遠藤委員長）
  - 今は初期なので、操作性の話が多い。現実的に士業であれば個人情報も扱うので、共用サーバに入れるか、という問題もあるし、使ってもらいながら、士業の使い方を探っているという状況。決まった時点で、その時点でセキュリティレベルを考えようと思っている。
- セキュリティは自前で実施することを考えているか。（江連）
  - セキュリティに関しては、リスクアセスメントをした上で考えている。ISMS を社長自ら実戦しているので、内容はわかっていた。
- 通常、セキュリティに目がいくのは後回しになると思うが、そこで敢えて、リスクマネジメントから考えられたのは、お客様からの心配があったのか。（川口）
  - まだ社会認知が進まない中で、どこまで使えるかから始まった。申請期間としては認証のセキュリティが求められるので、セキュリティはやらざるを得ない。（伊藤氏）

- ユーザから、煩わしいという意見はあるか。
  - 士業は自営業者なので、組織でないのになぜここまでやらなきゃならないのか、という意見も聞かれる。モニタとして使っていただいている士業独特のものなのか、一般的なものなのかはまだわかっていないので、稼働しながら把握しようと考えている。
- 安全代として、サービスを高い値段で売りたいということは考えていないか。（江連）
  - ISMS の認証を取るだけでも費用がかかり、安全代を上乗せせざるを得ない。士業は自営業者であり、安全に対してもお金を払える人ではないかと考えている。個人では安さが一番になるだろうが、ターゲットを個人に置いている場合、料金はなかなか引き上げられないだろうと考えている。安全対策を含めて提供できる料金設定を既に行っている。安全性にニーズが無かったとすれば、機能性を高める方向性に向けられる。（伊藤氏）
- 信頼性担保のための第三者の認証等へのニーズはあるか。（江連）
  - 士業向けを考えると認証を受ける必要はあると考えている。要求事項がかなり高いので、中小・零細であれば登録までにしばらくかかると思う。（伊藤氏）

3　株式会社つうけんアドバンスシステムズ様によるビジネス取り組み内容のご紹介

<< 講演 >>

- 250 人ぐらいの会社。北海道での仕事は減っており、従業員は、8 対 2 で首都圏に寄っている。
- 社長がクラウドと聞いて刺激を受けたことがきっかけでクラウド事業を開始。しかし、実際に投資でビジネスをできるかというと難しい。先行で大きな開発はできないので、補助金を受ける。官公庁向けの財務システム受託が主であり、パッケージでできるビジネスがない。
- SaaS モデルによる公共ポータルの開発を行っている。2 年前からシステム化したいというニーズがあった。委託料はあまりない中で、ニューメディア開発協会の補助を受けた。基盤の設計から始めている。
- 年間申請数 3,400 位。電子申請を SaaS 化できないかという要望があった。官庁よりのサービスの方が受け入れられやすい。これから機器を購入し、エレクトロニクスセンターに設置予定。
- セキュリティ対策については、札幌市から要請が来ている。ID・PW だけでは足りないレベルの認証が求められている。また、組織としてもデータにすぐにアクセスできない運営体制を求められている。
- 事業者が使う電子申請も考えている。業者登録はオンラインシステムで実施。2 年に 1 回しかない。一般事業者には ID・PW で提供しているが、特に問題ない。
- 個人情報管理は、一般的なものであまり触れないでいる。
- 年に 1 回しか電子申請しないので、IT をスムーズに利用できるかどうかの方が問題。

- ローカルクラウドーキント雲と呼んでいるーは、大手に乗っからないと負けると考える。中小規模は、対応すべくサービス化していないといけない。
- サービスの統合化の話が出ている。北海道でも 30～40 事業者に集約していくとのこと。競争相手は限られる。自治体相手なので、長くは維持できると考えている。

<< 質疑応答 >>

- ローカルクラウドの範囲はどう考えているか。(川口)
  - まずは札幌と考える。社長は、NPO 札幌市 IT 振興普及推進協議会の理事長をやっている。単なる受託企業では終わらず、新しいものを打ち出していこうという意識が強い。テクノパークの協議会理事長もやっているので、連携をしながら行っている。(中島氏)
- 経済産業省の方の話では、クラウドでうかうかしていると、米国にやられるだろうと指摘している。戦える土壌を作る必要があると認識しているが、なかなか難しい。札幌市の同業の方も同じような認識でいるのか。(遠藤委員長)
  - どちらかというと自身が盛り上げている。3 社のコンソーシアムを構築しており、いずれもパッケージを持っているので、SaaS に展開していきたいというニーズがある。SaaS でやっても営業の方法は変わらない。電話会社を選ぶほど簡単ではない。業務系アプリケーションは信用など、複雑に絡み合って決まる。補助金をいただいているが、大赤字になるだろうと思っている。1 ヶ月立ったのに契約前でお金が使えないので困っている。(中島氏)
- なぜポータルサイトの構築から始めたか。(池田)
  - 申請上の名目が大きい。単体 SaaS を考えていたが、ポータル的にしないと申請が通りにくい。官公庁でも LGWAN 等で SaaS があるが、定額給付金のシステムが初めて。業務系ではあまりこういう動きはない。政令指定都市の会合があるので、上手く他にも展開できるとよい。(中島氏)
  - 消防局では契約で心配な面があるので、覚書を交わしてほしいという意見もあった。使えるものになるのか。(松田氏)
  - 財団が主体となって申請し、補助金を得た。通常、採算が合わない場合は辞めてしまうが、多くの自治体向けということもあり、今回は 1 年やってだめだから辞めましょう、という訳にはいかない。(中島氏)
  - ユーザが直接契約しない。従来のシステムでは、調達面では専門家が入っていたが、SaaS の場合は、ユーザ部門が直接サービスとして契約してしまう。変更管理もなされずにどんどん変わって内部統制的に問題になってくる場合もある。今後、見直しがなされるのではないか。セキュリティの確保という点では、問題になってくる。(遠藤委員長)
- セキュリティ対策の状況は。(平木)
  - システム的な面で言うとこれからというのが実情。(中島氏)

- 財団が申請者なので、セキュリティの責任がある。（松田氏）
- もともとこの施設に設備があるので、利用しようと思っている。（中島氏）

・ 新しいビジネスが必要となってくるか。（平木）
- 設計そのものは問題が出てくるだろう。IC カード部分でどう行うかいろいろ課題が出てくるはず。開発自体は来年 2 月まで、サービスは 4 月インで考えているが、その間にユーザとやり取りがあるだろう。（中島氏）
- 札幌市のネットワークが強固な形なので、専用回線を引き込んでやっていく形となるだろう。札幌市自身も電子入札をやっており、完全に ASP でやっている。参加者も IC カードを持っている。（中島氏）
- どの程度行政事務が SaaS 化できるか次第。住民基本台帳を中心とした業務が多いので、難しいかもしれない。（中島氏）

・ アライアンスの意向はあるか。（江連）
- 研究会の 60 社にはアピールしている。札幌市の SaaS 系の事業活動と歩調を合わせながらやっていきたい。受託系が多くなってくると思う。もう少し NGN のセキュリティ部分の動向が見えてくるとよい。（中島氏）

・ 仮想化は実施されているか。（平木）
- 社内的には徐々に始めている。昨年度の検証でもやっている。（中島氏）

・ パブリックで安くて自由に使える環境が米国から来ている段階だが、使ってみようと思うか。（遠藤委員長）
- Amazon 等を使ってみたが、自分のものではないため、難しい面があった。採算性を考えて使った方がよいと考える。きっちり使う仕組みがあれば使うが。短期間であれば自前でリスクが少ない方を使う。（中島氏）

4　クラウド/SaaS 時代のセキュリティに関する意見交換

・ 普及シナリオについて、こんな簡単にはいかないという印象か。（江連）
- アンケートの対象にもよるが、ICT に慣れた方々が回答しているのではないか。中小・零細企業や一般企業の方は、対外漏洩して事業継続にダメージを与えるような情報を持っていない。コストパフォーマンスに傾倒するのではないか。弊社としてもそこまでは対応できないので、ある程度セキュリティにお金を払っていただける人をターゲットとしているが、クラウド/SaaS の社会認知が進む中で、セキュリティよりも、安くしてくれという流れに行く方が現実的ではないか。（伊藤氏）

・ 大規模クラウド・ビジネス　対　中小クラウド・ビジネス　という形があり得るか。浸透していくシナリオが描きづらい。セキュリティが足りないという意見もあるが、そんなに心配していない印象もある。（川口）
- 問題は、サーバが外に出ていて、ポートが外に開放されている部分は脆弱性が高い。それを踏まえた上で、インハウスでやる部分と、外側で持つ部分につい

て、資産価値を分けるのではないか。基幹系は中で持ち、情報系は外に出す、というのは大企業だけではなく零細は別としても中小企業レベルは同じではないか。基幹系は中で持ちたい、その事業者で責任が持てるかどうか。自前サーバが落ちてもデータは無くなるが、漏洩はしない。基幹系については、営業時にユーザの話を聞くと外に出したがらない傾向が強い。（伊藤氏）

- やはり基幹系は外に出さないのか、中で持っていても対策は大変、内部犯行もあるので出して責任を押しつけたいのか。（川口）
  - 経営規模にもよる。自営・零細関係は、今現在 PC も使っていない。何が基幹系かというレベルでは、入り口が SaaS であるということで入ってくる可能性はある。敷居は低いので。すべてオンライン化で使う方向性もある。現在、クラサバ系で使っているようなレベルであれば、基幹系と分けて持ちたいという流れがある。大手もそのような形で考えているのではないか。（伊藤氏）
- 連携をどうするかという問題も出てくると思うが、クラウド・インテグレーション的なものが出てくるか。（川口）
  - 連動と言われても、基幹系と連携するものは出さないのではないか。自社のケースで言うと、社内様式を函館と共有するには、外に繋いで最新版の社内様式を取れるが、会社資産として価値が低いものはこのような形で使える。基幹系の重要な情報は本社ですべて管理しており、各支社で使っているのはそこまで重要ではないので、SaaS 的に使える。ユーザの視点では、使い分けは十分できるのではないかと感じる。（伊藤氏）
- そのモデルを中心に考えると、認証部分以外にリスクとして何を考えるか。（川口）
  - リスクアセスメントの上ではかなり議論を重ねる。月に 1 回定例に加え、臨時の検討も行う。なりすましもそうだが、最も懸念するのは、アプリにもよるが、管理者が ID・PW を管理・発行できる形のソフトウェアなので、見えないところで使っている方がいる。ユーザ側の管理者がミスったところで、事業者の責任にされると厳しい。現実には可用性を考えると、ユーザ側の主管理者が、ユーザの ID・PW を振る。ユーザ側が正しい管理をしてもらえるかどうか。とは言え、器は事業者が提供している場合。どこまで責任を取るべきか。これは、契約に盛り込むときに悩んだところである。SLA でどこまで見られるか。（伊藤氏）
- セキュリティ対策で苦労する点はあるか。（川口）
  - 一番重要なのは電子請求をするところ。センシティブ情報を載せるところではない。A さんの利用料は幾ら等という、基幹系との連動するところ。SaaS でやるかどうかという問題。そうすると相当のセキュリティが必要になる。介護系は、家族情報、病気の情報も含まれるので、対策は事業者側で絶対的にやらなければならない。しかし、やり過ぎてもコスト的な問題が発生する。電子請求の部分で SaaS、技術とコストの状況を踏まえて検討していくという方向になる。

外側にデータを置いた場合に、ちゃんと使っていただけるかどうかは気になる。内部犯行もあるが、トレースは可能。インハウスの場合論理的に何かできる訳ではないが、回部の場合、何者かがいたずらをする可能性もある。やればやるほどコストは上がるので、コストを支払える体力はない。（伊藤氏）

以上

講演録（株式会社 HARP）

日時	2009 年 10 月 2 日(金)10：00－11：30
場所	札幌グランドホテル本館 3 階「松風」
講演タイトル	「株式会社 HARP における事業内容のご紹介」
講演者	株式会社 HARP 常務取締役　企画営業部長　　金川 泰之　氏 プロジェクト推進部　マネージャー　　山内 康史　氏 プロジェクト推進部　サブリーダー　　米倉 研太　氏

講演概要

HARP 社の事業内容についてご説明いただき、セキュリティ確保の考え方、ユーザのセキュリティに対するニーズ、自治体と民間のニーズの違い等について意見交換を行った。クラウドという技術はユーザから見えるものではなく、ユーザから見える事業者の信頼が重要であるという指摘が得られた。

講演の要点

1　HARP 社の事業内容のご紹介

・ 第 3 セクターとして設立。官民連携して役員を選出。
・ 主要株主は、北海道、NTT 東日本、北海道電力、北洋銀行等。
・ H15 に HARP 構想、e-JAPAN を契機に自治体の行政化の流れがあった。実用化していることが特徴。
・ 目的は 3 つ：住民サービスの向上、行政サービスの効率化、地域経済の活性化
・ SOA を活用し、自治体向けアプリケーション（電子申請、施設予約、電子調達）を ASP で提供している。自治体で各システムを保有しているが、システムが複数あることで重複部分があるはずということで、重複部分を取り上げながら共有し、分割・提供することに成功した。各部品については北海道の地盤企業　26 社に分割発注している。アプリケーションも別のベンダに発注している。
・ 北海道及び HARP 協議会で方針決定、実行にあたり地場の IT 企業が集結している。
・ SaaS への移行は 2 年前からロードマップを描いている。ASP は 2000 年頃から騒がれていたが、あまり普及しなかった。ハード、ソフト、ネットワークの環境が整っていなかった。特にネットワークの問題が大きい。現在は、青森、大分、宮崎にも提供している。
・ 情報については、自治体が保有する情報の一部を持っている。セキュリティについては、自治体そのものの業務を効率化するサービスが本業だが、どうしても関わってくる。自治体の課題が浮き彫りになってくる。自治体では専門知識を持つ人材がいない。情報政策課・企画課にも人がいなく、また担当者は何十年も同じ部にいる訳ではない。民間と異なり、お金だけでは進まない。査定をする部分が落ちる。民間と異なる普及シナリオ

が必要と考えている。

- もう 1 つの課題は財政難。お金をかけたくないが、効率化はさせたい。
- 大手外資系からも話が来る。しかし、民間企業向けの話ではないか。ハード的な部分のシェア、仮想化は大歓迎だが、自治体に言ってもわからない。個人的には、クラウドは入り口だけ。ユーザが見えるのは HARP 社だけ。直接エンドユーザにクラウドがいく訳ではない。間に入ってビジネスを見ることが、クラウドの究極の形ではないか。 現在、HARP コントローラー1.0 から 2.0 に移行中だが、複数のデータセンターをどう取りまとめていくか。その時々に応じて最適な形をもっていくか。セキュリティをどうやっていくか、自治体業務では、様々な情報がある。クラウドには法的規制もまだない。ワンクッション、ツークッション必要であろう。総務省、経済産業省とは別の部分の検討が必要であろう。
- これまでキャッシュアウト型でやってきたが、自分たちで持っているアプリは 1 つだけではない。差分の吸収の仕方が難しい。基本路線を 1 本に絞って差分を少なくするか、そこで差別化をどう図っていくかが重要。
- セキュリティは詳細な部分までは話せないが、LGWAN-SG は LASDEC に準じたセキュリティレベルを確保している。セキュリティを確保している事業者の力を借りながら、実施している。入り口は同じなので、あとはユーザが何を使うかの問題。基本のセキュリティは一律で、セキュリティパックがあるのが理想。

2　質疑応答

- 総務省のシナリオ、経済産業省のシナリオと合わない部分とはどこか。（川口）
  - 管轄省庁が違う。自治省系/ソフトとハード系という印象を受けている。経済産業省は箱を作るが、ソフトを作るのが総務省というイメージ。内閣府の IT 推進の考え方も違う、住基カードと何が違うのか等。（金川氏）
- 電子自治体は横展開しやすいと思っていたが、それでもカスタマイズ部分があるのか。さらに民間だともっと難しいと考えられるか。（川口）
  - 自治体は最初にはやりたがらない。どこか 1 つ入ると、一気に流れていく。バックオフィス系では業務が全く異なる。フロント系は入りやすい。福祉等は異なる条例を持っているので、どこかが改革して経済的効果があったかというのが示せると、他の自治体にも進んでいると考えられる。（金川氏）
  - 民間でも事例が出てくることで、普及が進んでいく。（遠藤委員長）
  - 民間は儲けが重要。行政は予算執行型なので考え方が異なるかも知れない。（金川氏）
- セキュリティが差別要因になるか。（川口）
  - 入り口が HARP に入ったとき、オプションとしてはメーカー指定、機能指定でくるかもしれない。料金体系、手続きが同じであることで判断がしやすい。（金川氏）

- 資料 P22 の部分（SI のクラウド化＋セキュリティ機能の付加）に需要はあると思うか。（川口）
  - そこが一番だと思う。どこを信用するか、信用に値するところが見つかればよい。淘汰が進む。他は傘下に入ってくる。HARP が言っているのはソフトウェアハウス系、ベンダ系、大手だけでできない部分がある。汎用機からクラサバに変わってもまだまだ大きい。更改する費用もメンテナンス費用も持てない、分割して利用する。パイの中でどれだけ取れるかになるとコスト競争になってくる。（金川氏）
  - 米国のような体力勝負で攻める人たちが出てくるが。（川口）
  - それに乗る人もいるだろうが、ごく一部ではないだろうか。民間よりもパブリックの方で普及が進むのではないか。ハイブリッドの話もあったが、プライベートで構築というのもある。小さいところは大手と話ができない。（金川氏）
- HARP 構想の中でも、バックオフィスは個別の業務が多いので難しい。民間でも同様。両極で進んでいくと考えるか。（遠藤委員長）
  - バックオフィスも同様に共通化。フロントに近い部分から徐々に手をつけていき、不安がなくなれば徐々に進展する。（金川氏）
  - 自分のデータを出したくない、という傾向はあるか。（遠藤委員長）
  - セキュリティに関しては、民間と異なるのは、原本管理は現場で持つ必要があること。法整備が進んでいないので抜け道はたくさんある。預けることの不安より、預ける楽さの方が大きい。住基情報になってくると避けて通ることはできない。データ銀行のようなものができれば、使うものだけ提供できるが。使い方、情報漏洩など運用については使う側の責任となってくる。原本がどこかにあり、使うときだけサービスというのがクラウドの姿ではないか。（金川氏）
- 原本管理も行っているのか。（平木）
  - 行っている。（金川氏）
- 他地域へも展開しているのか。スケーラビリティは。（平木）
  - 宮崎と大分。広げたいと思うが、なかなかスムーズにはいかない。そもそも電子申請では、収納や書類を取りに行く部分があり、そもそも完全電子化が進んでいない。ASP 事業者なので、独自の考えとして展開できる。（金川氏）
- アンケートではセキュリティが大事だと言われるが、ユーザの話を聞くと、実際はあまり考えていないようだが。（川口）
  - 紙の管理もずさんなのが現状。きちんと教えることが必要。ユーザとは対面で確認を取るが、本当に理解しているかはわからない。責任問題だけ。入札に参加してくる企業は、対策はしていると言うだけ。LGWAN-ASP は LASDEC の厳しい規定があるので、ハード、ソフトを含めて対応している。（金川氏）
- 世の中の認識が進んで、危険とそうでない部分がユーザでもわかってきたとして、セキュリティに対するニーズが顕在化した場合に、どこに注力して手当をしていけばよいの

か。（川口）

- 自治体から言うと、改ざんが問題ではないか。大きなトラブルはまだないが、原本との照合を気にされている。また、まだ紙でしかないが外国人の問題もある。地方によって字が違うのでデジタルアーカイブできない。同じものが使えるか、改ざんされないか。漏れるというより、改ざんされないかが問題ではないか。（金川氏）

・ 紙のビジネスに対するニーズはまだあるか。（平木）

- 自治体は紙の文化なので、最終的には紙で持ちたいという要望は強い。HARP に頼めば難しいところを全部やってくれるというところが大事。信頼をどう持ってもらえるかが重要。（金川氏）

・ 電子私書箱や IC カードはどこまで進むと考えるか。（平木）

- IT 推進室とも話をしたが、どうやって進むのかわからない。もう進まないかもしれない。結局、何に使うのかが明確になっていない。人生のイベントに使うにせよ、数回しかない。使ってもらうためのコンテンツが必要。（金川氏）
- 実証実験も行われており、コンテンツを詰め込んでいるが。普及していくとまた問題も出てくるだろうか。（遠藤委員長）
- ハードでがちがちではなく、ソフトで自由にできる部分が増えるとよい。ハードに依存すると、結局コストに反映される。LGWAN もがちがちでセキュリティボックスがいろいろついてくる。民間はそこまで重たくないと思うが。そこでセキュリティも確保できればメリットとなる。（金川氏）

・ セキュリティのオプションとして、どんな機能が考えられるか。（川口）

- データの受け渡し方法、暗号化等。バックアップ。オプションはあるだろう。安くてよいものから高いレベルのものまで。自治体でも意識は異なる。（金川氏）

・ 安心してもらえるのは実績がたくさんあること、LGWAN-ASP の規定に準拠しているなど、どういうことがあるか。（遠藤委員長）

- 資格はみんな持てる。実際にどう使っているか、実績が大事。フロント系だけではなく、共同化を上手く回している実績を買っていただいている。必ず必要。短期ではできない。あとはどこまでコミュニケーションできるか。データセンターも見ていただいているし、いかに自分の会社を知ってもらえるかが大事。大きくなりすぎても難しいのではないか。こういう会社がたくさんあるのが理想。1 社でやれる規模ではない。（金川氏）

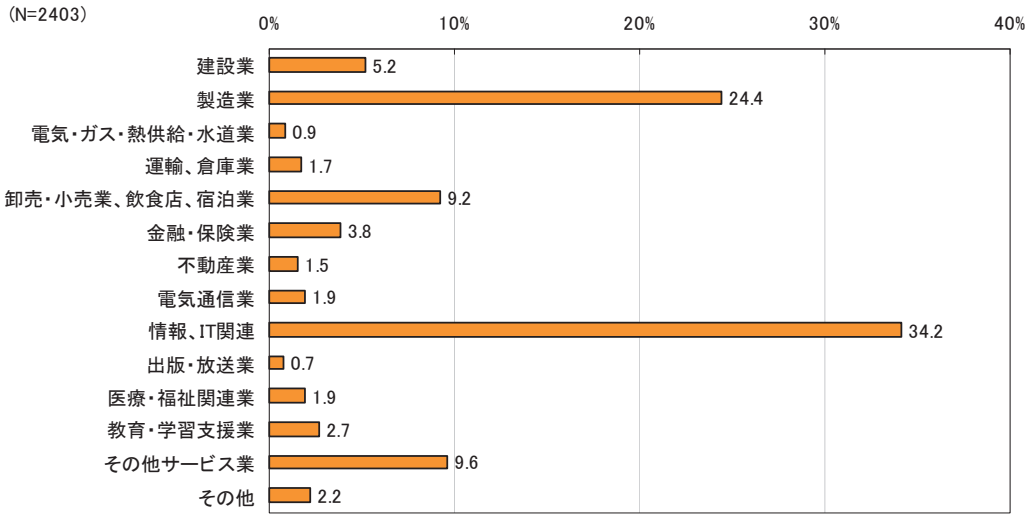
以上

付録 III　アンケート単純集計結果及び調査票

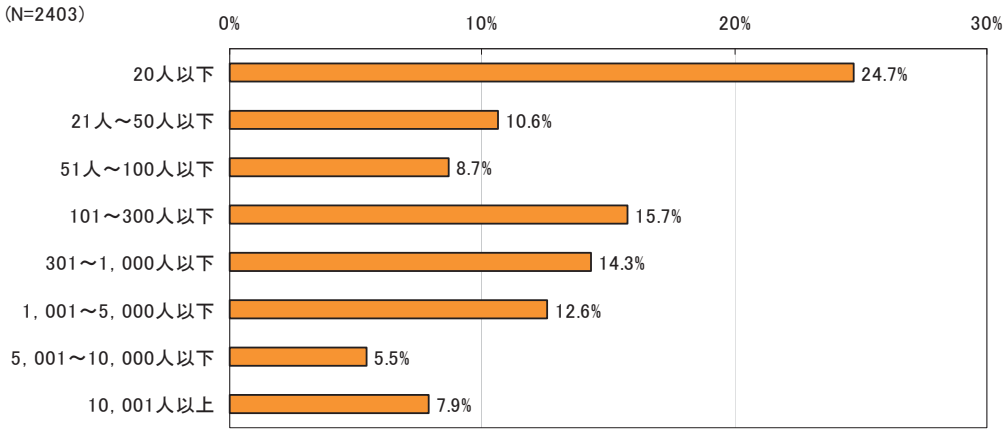
アンケート単純集計結果

【第 1 次調査：あなたの勤務先の情報システムに関する調査】(全対象者)

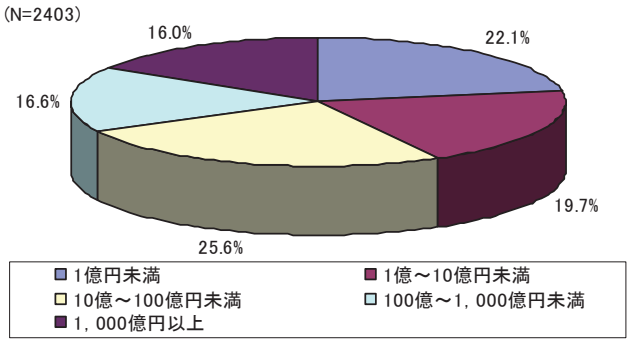
F1　貴社が属する業種は次のうちどれですか。当てはまるものを 1 つお選び下さい。



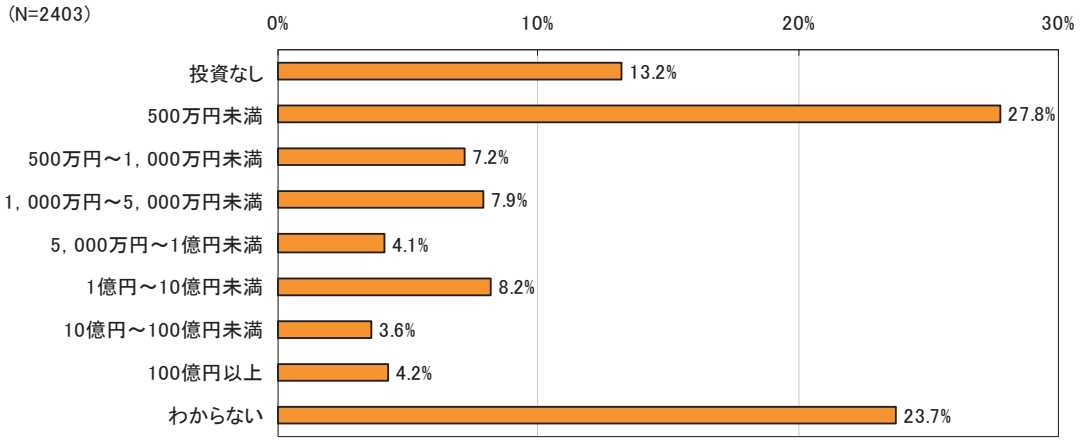
F2　貴社の従業員数は次のうちどれですか。当てはまるものを 1 つお選び下さい。



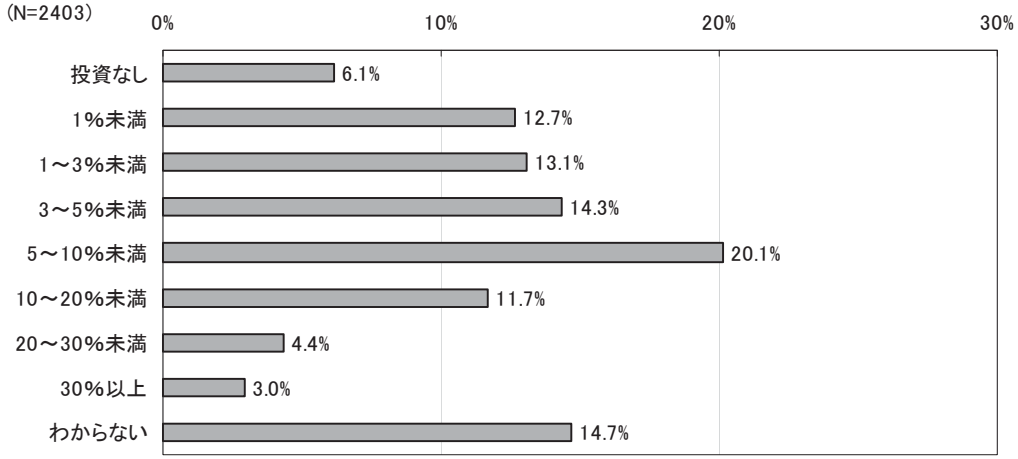
F3　貴社の売上高は次のうちどれですか。当てはまるものを 1 つお選び下さい。



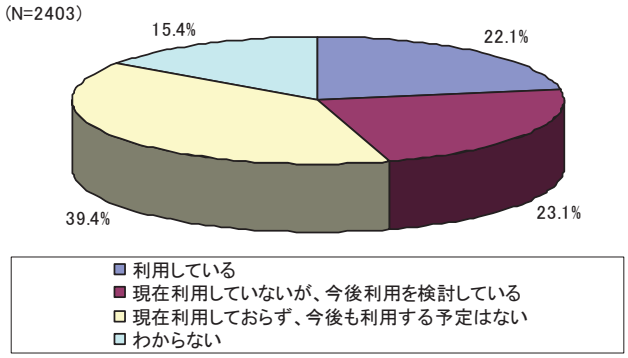
F4　貴社の直近年度の IT 投資額（予算）について、当てはまるものを 1 つお選び下さい。



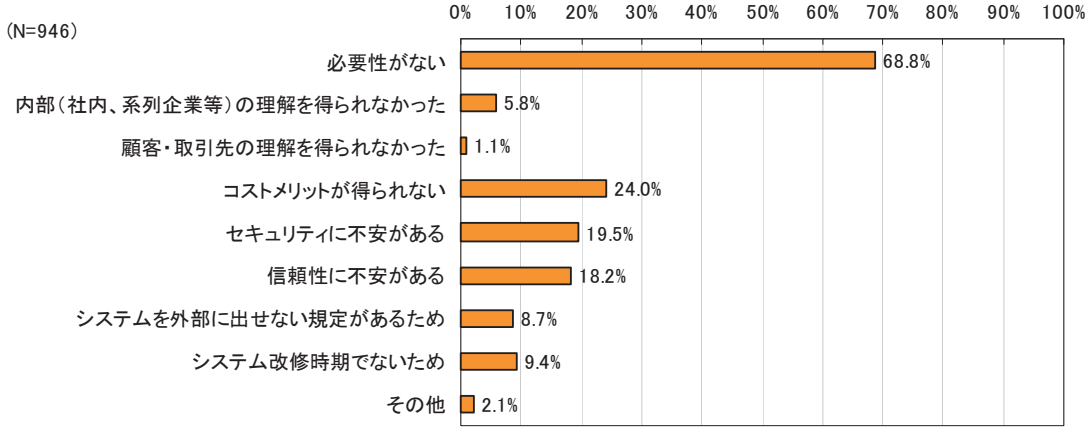
F5　F4 の IT 投資額に対するセキュリティ対策費用額の割合について、当てはまるものを 1 つお選び下さい。



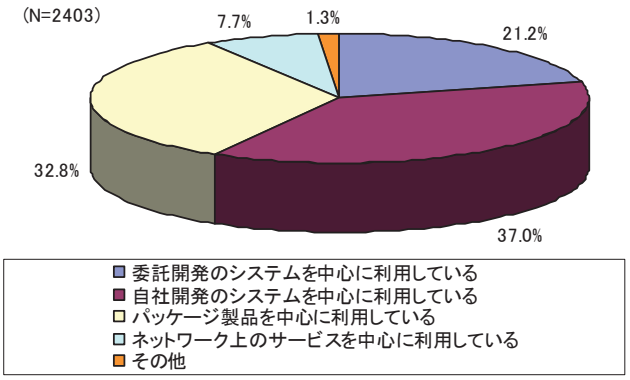
Q1　貴社の情報システムにおいて上記のようなネットワーク上のサービスを利用していますか。当てはまるものを１つお選び下さい。



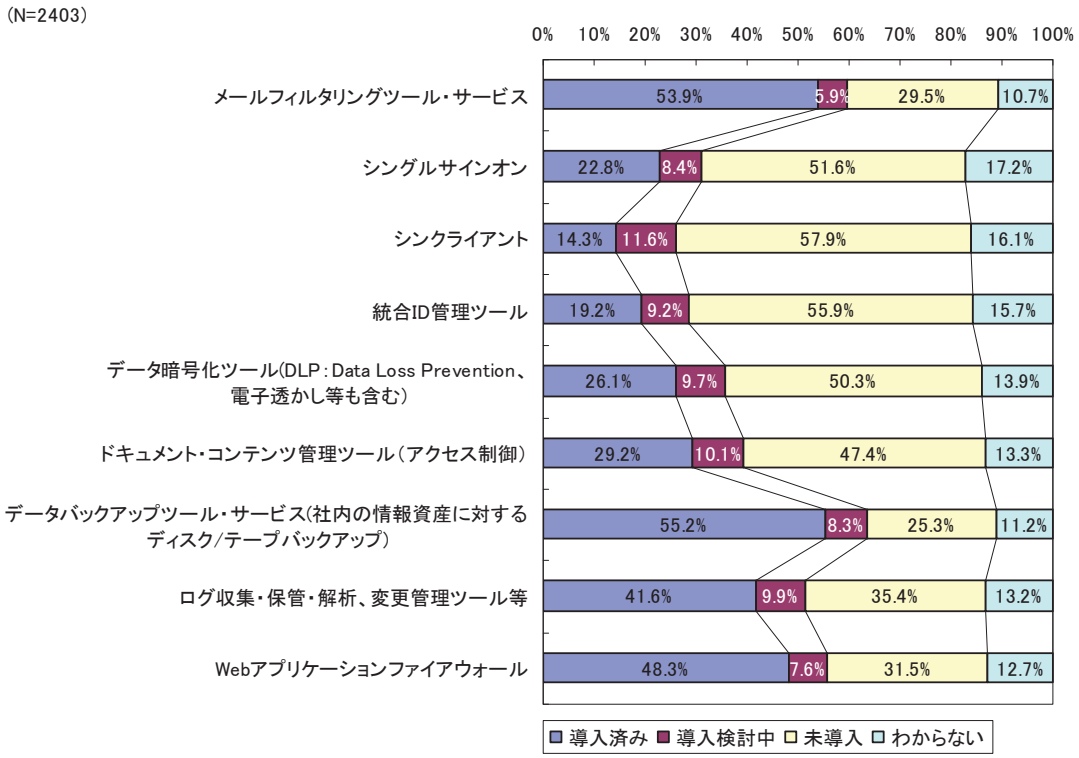
Q2　貴社で上記のようなネットワーク上のサービスを利用していない理由は何ですか。当てはまるものすべてお選び下さい。【Q1 で「3. 現在利用しておらず、今後も利用する予定はない」と回答された方のみ】



Q3　貴社における現在の情報システムの状況について、最も近いものを１つお選び下さい。

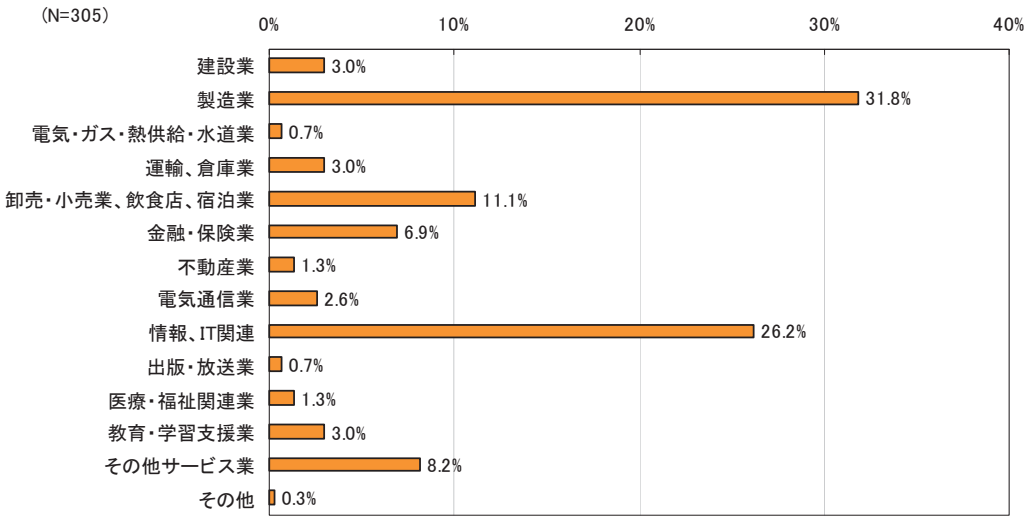


Q4　貴社における以下の各情報セキュリティ製品・サービス（ネットワーク上のサービスに限らず）の導入状況をお答え下さい。

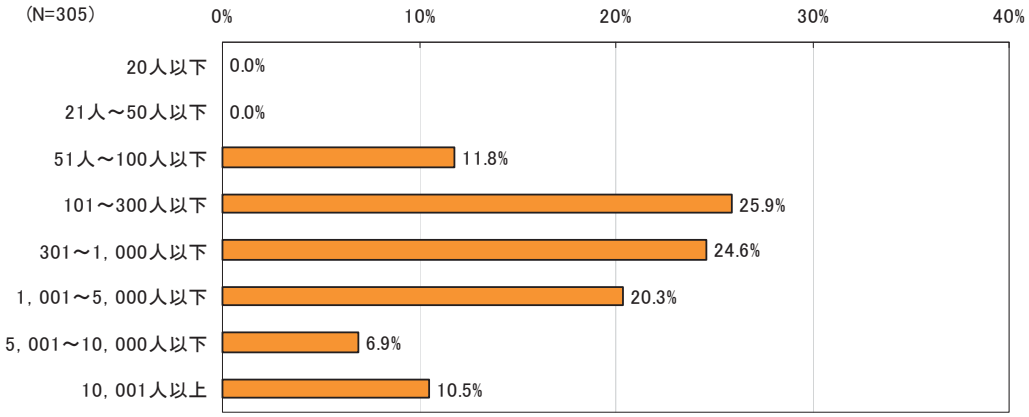


【第 1 次調査：あなたの勤務先の情報システムに関する調査】(第 2 次調査対象者のみ)

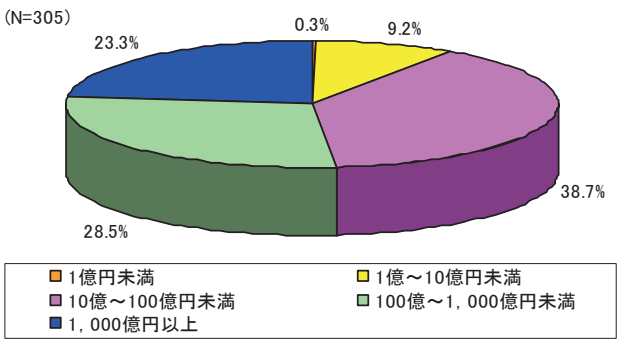
F1　貴社が属する業種は次のうちどれですか。当てはまるものを 1 つお選び下さい。



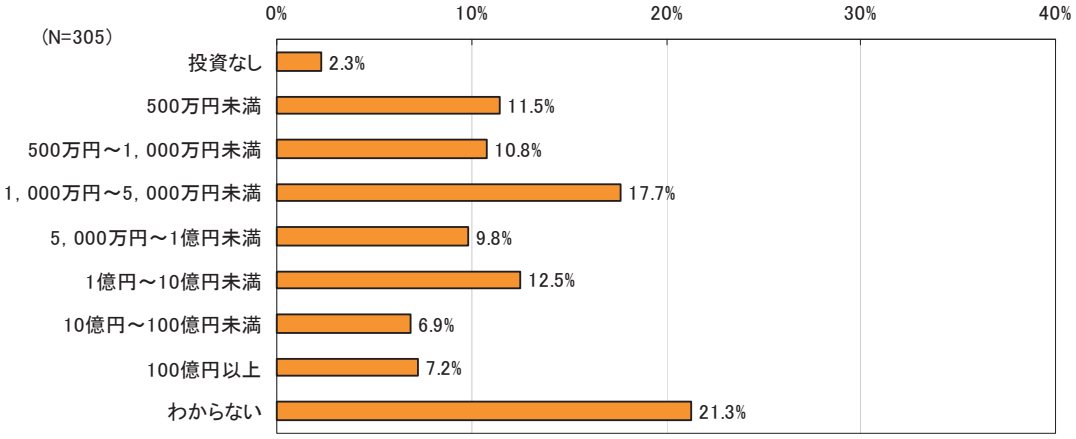
F2　貴社の従業員数は次のうちどれですか。当てはまるものを 1 つお選び下さい。



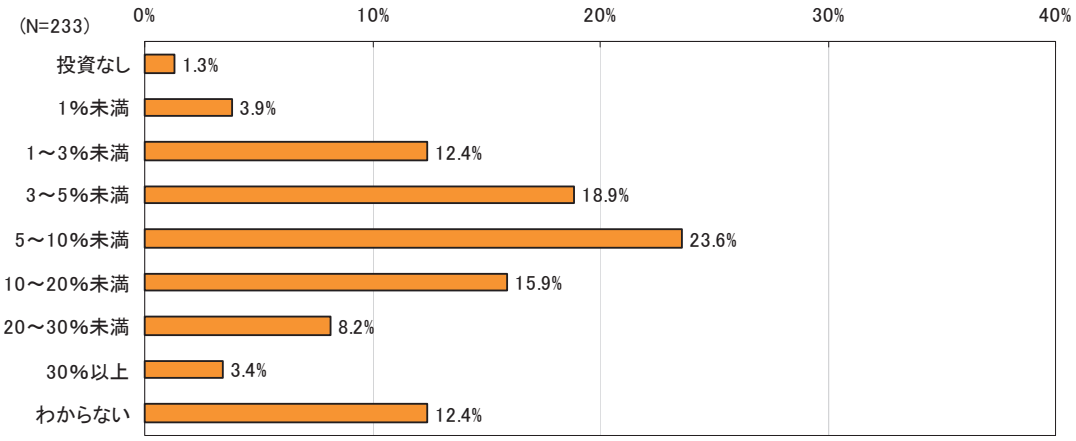
F3　貴社の売上高は次のうちどれですか。当てはまるものを 1 つお選び下さい。



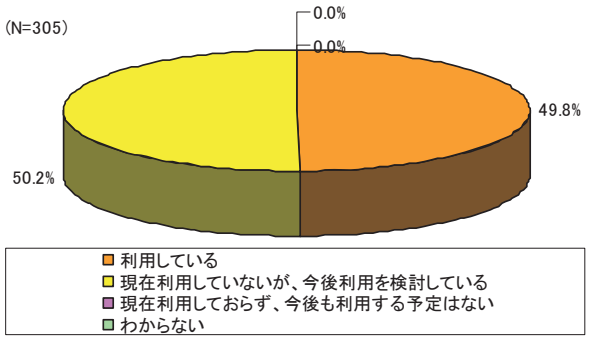
F4　貴社の直近年度の IT 投資額（予算）について、当てはまるものを 1 つお選び下さい。



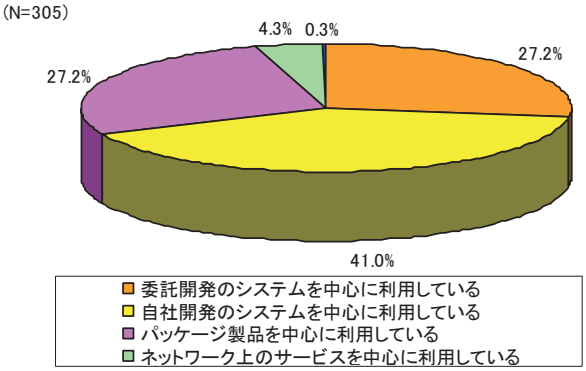
F5　F4 の IT 投資額に対するセキュリティ対策費用額の割合について、当てはまるものを 1 つお選び下さい。



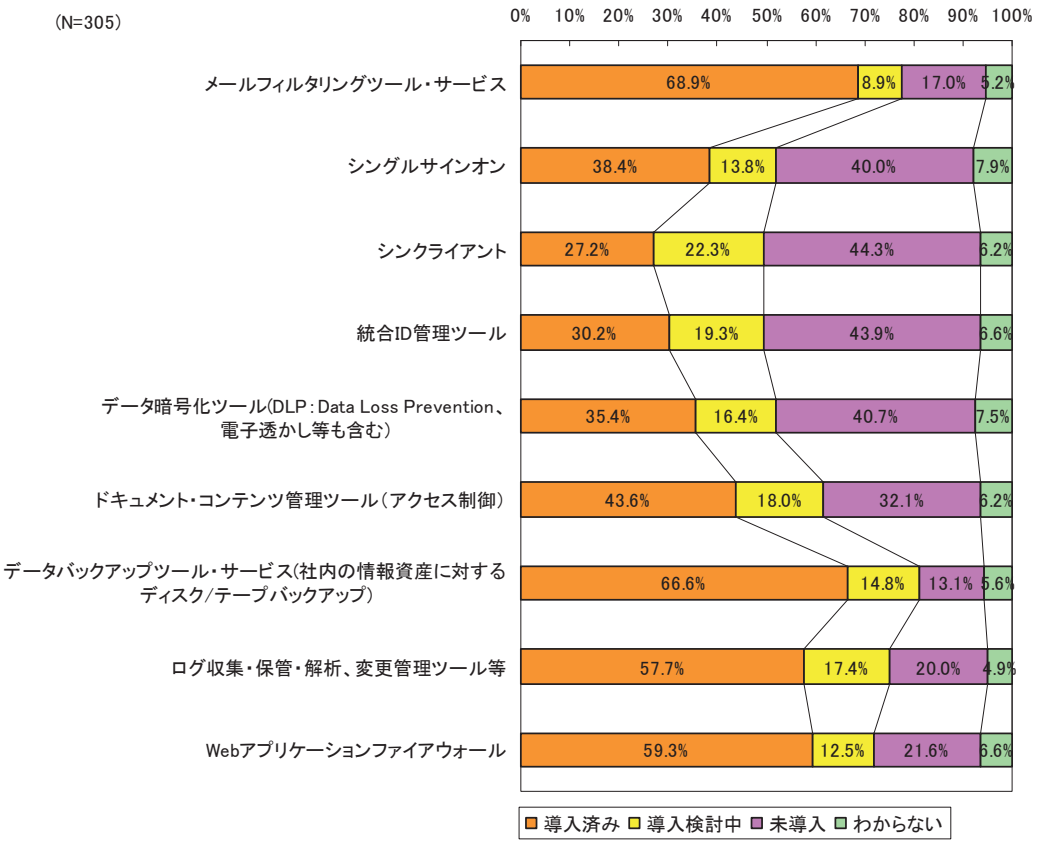
Q1　貴社の情報システムにおいて上記のようなネットワーク上のサービスを利用していますか。当てはまるものを 1 つお選び下さい。



Q3　貴社における現在の情報システムの状況について、最も近いものを1つお選び下さい。



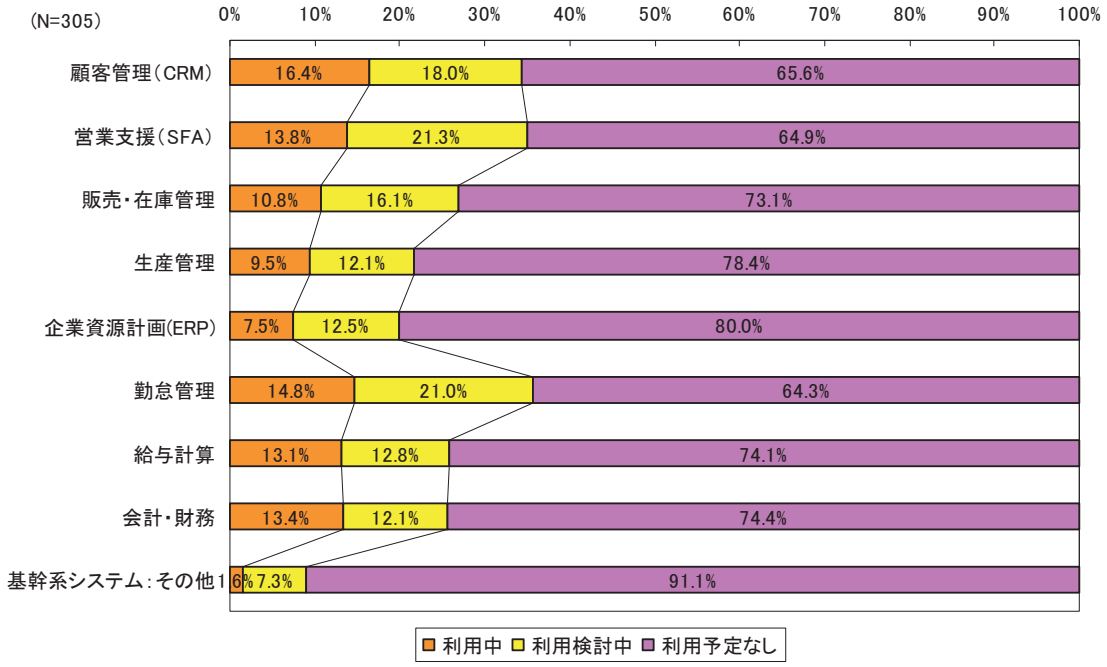
Q4　貴社における以下の各情報セキュリティ製品・サービス（ネットワーク上のサービスに限らず）の導入状況をお答え下さい。



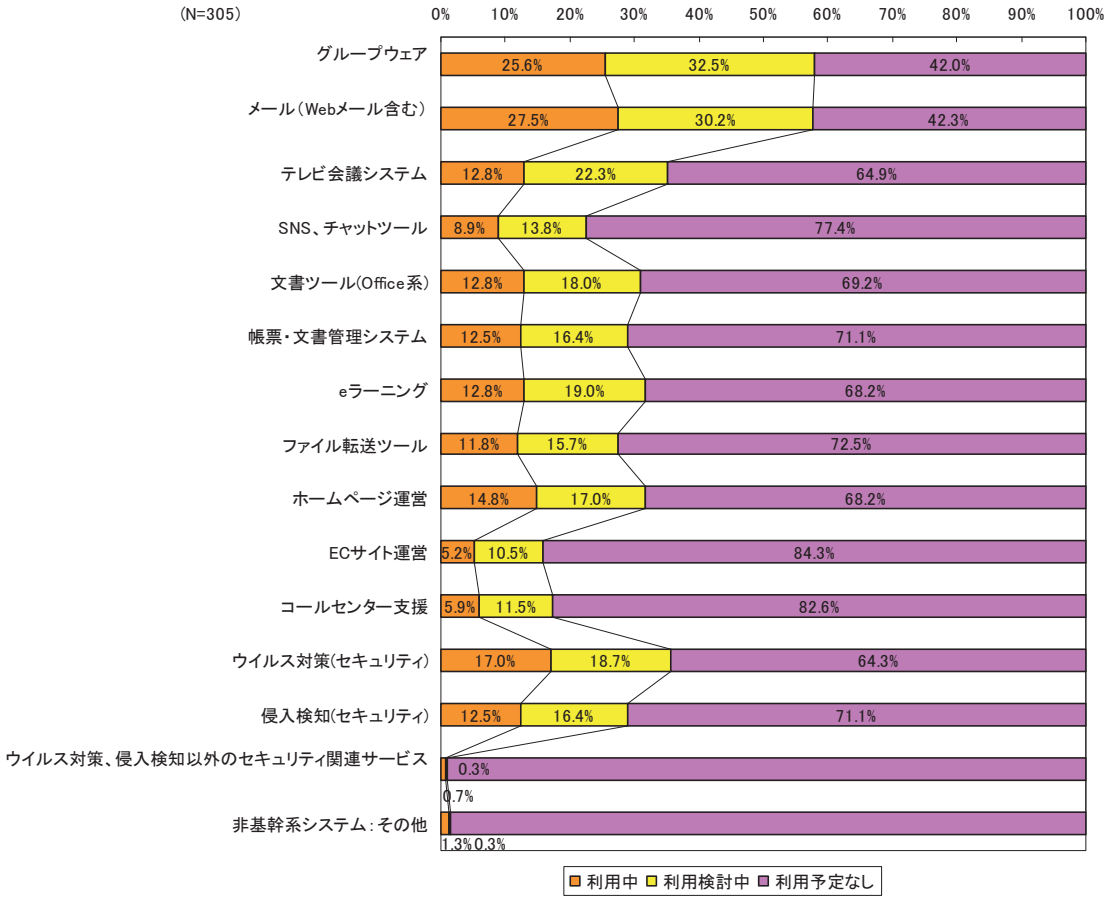
【第 2 次調査：クラウド/ SaaS 利用に関する調査】

Q1　貴社の各情報システムに関するクラウド/SaaS の利用（クラウド上に構築しているものも含む）状況をお答え下さい。【クラウド/SaaS 利用者、利用検討者】

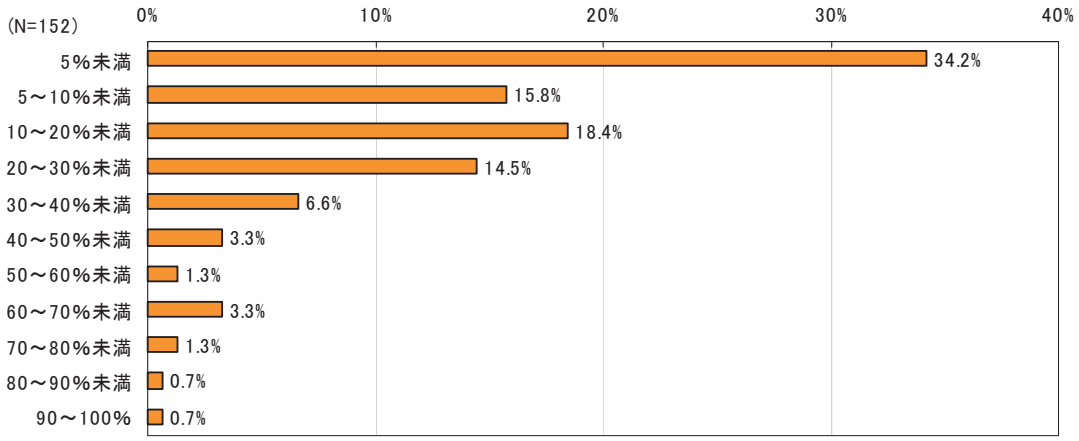
【A.基幹系システム】



【B.非基幹系システム】



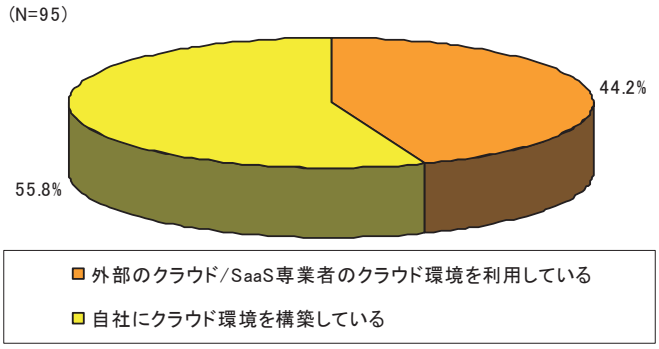
Q2　貴社の上記のシステムを含む全社の全情報システムにおけるクラウド/SaaS の利用割合はどの程度ですか。当てはまるものを 1 つお選び下さい。【クラウド/SaaS 利用者のみ、以下同様】



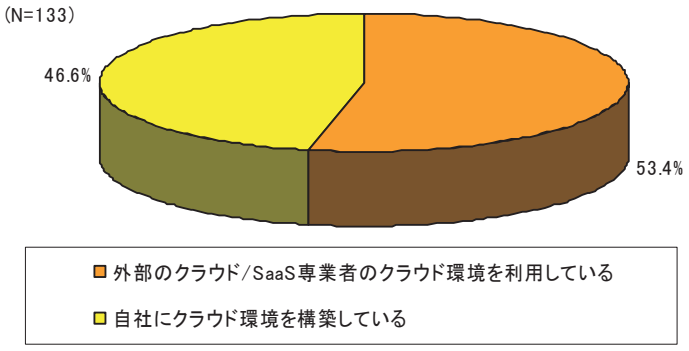
Q3　貴社ではクラウド/SaaS をどのような形態で構築、利用していますか。最も貴社の状況に近いものを 1 つお選び下さい。

※　Q1 で A、B 両方において「利用中」と回答した場合はそれぞれについて回答。片方のみ「利用中」と回答した場合は、片方のみ回答。

【A.基幹系システム】



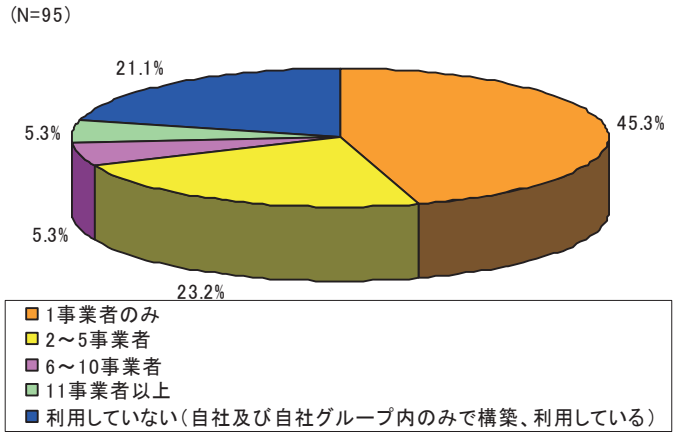
【B.非基幹系システム】



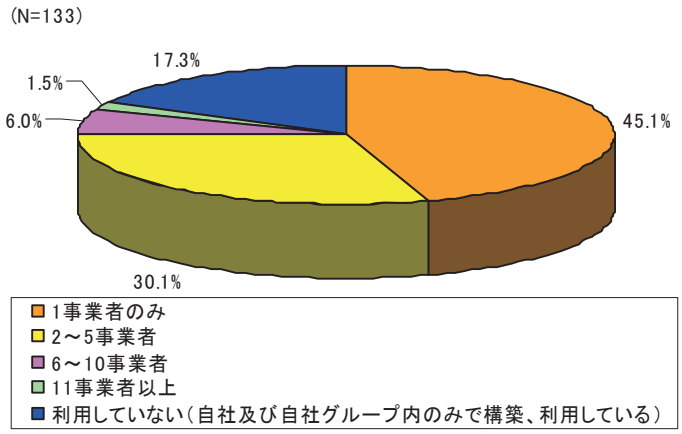
Q4　貴社ではクラウド/SaaS 専業者（直接クラウド/SaaS のプラットフォームやアプリケーションを提供する事業者、導入支援のみを行う事業者等は含まない）を合計何社利用していますか。当てはまるものを 1 つお選び下さい。

※　Q1 で A、B 両方において「利用中」と回答した場合はそれぞれについて回答。片方のみ「利用中」と回答した場合は、片方のみ回答。

【A.基幹系システム】



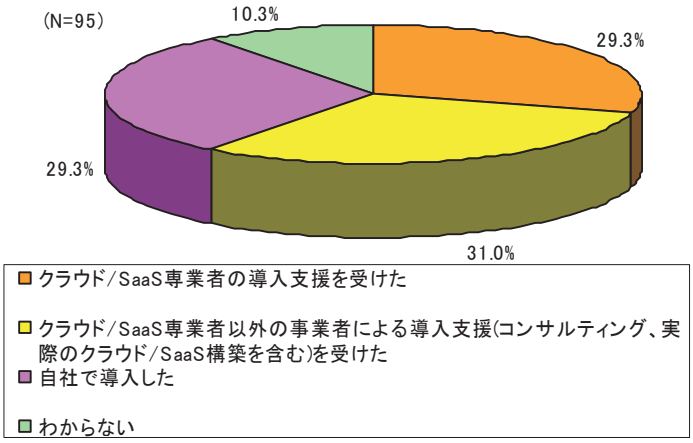
【B.非基幹系システム】



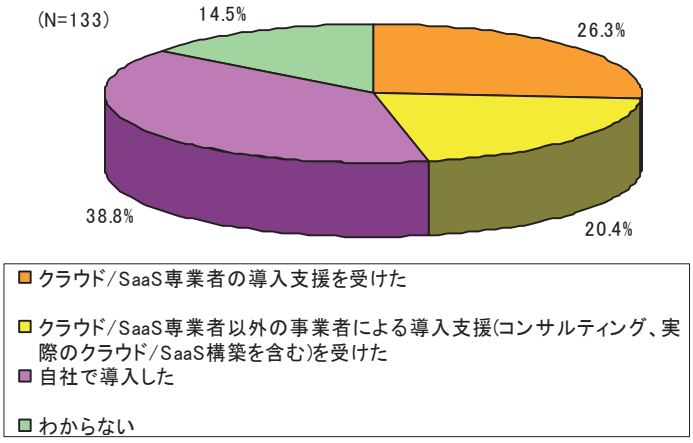
Q5　貴社でクラウド/SaaS を導入する際、どのように行いましたか。当てはまるものを**すべて**お選び下さい。

※　Q1 で A、B の両方において「利用中」と回答した場合はそれぞれについて回答。片方のみ「利用中」と回答した場合は、片方のみ回答。

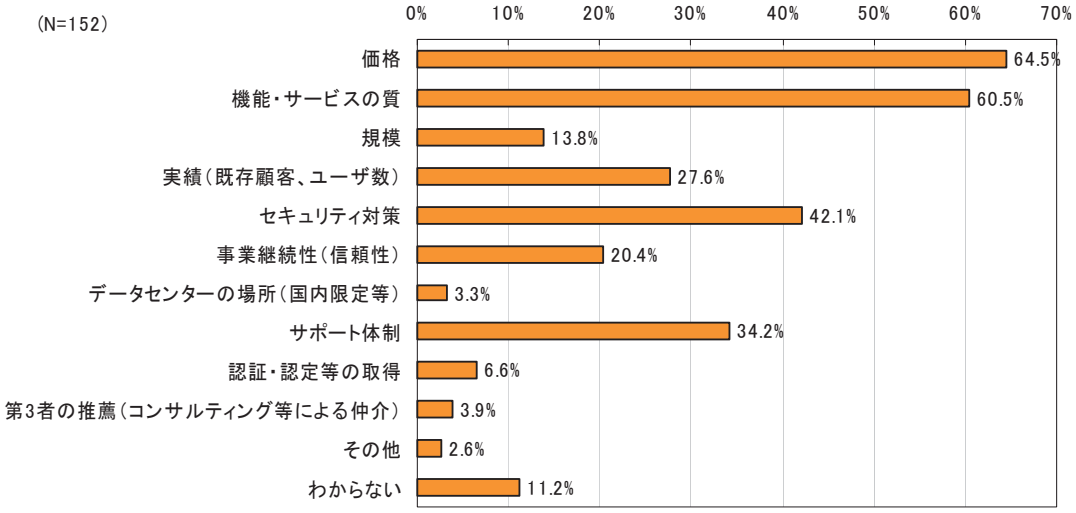
【A.基幹系システム】



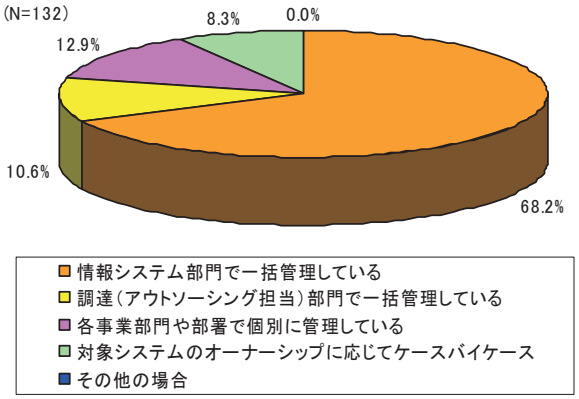
【B.非基幹系システム】



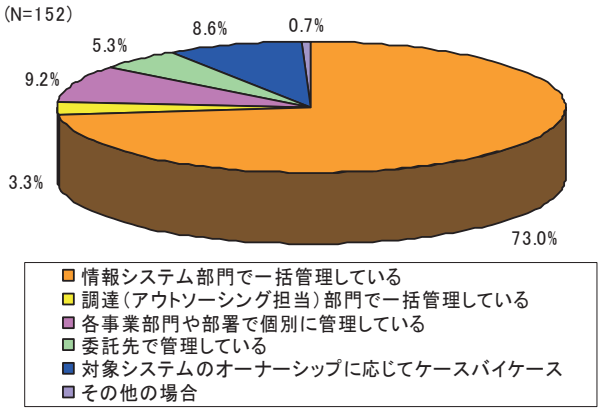
Q6　貴社でクラウド/SaaS を導入するに当たり、クラウド/SaaS 専業者の利用検討・選定において何を重視しましたか。当てはまるものを 5 つまでお選び下さい。



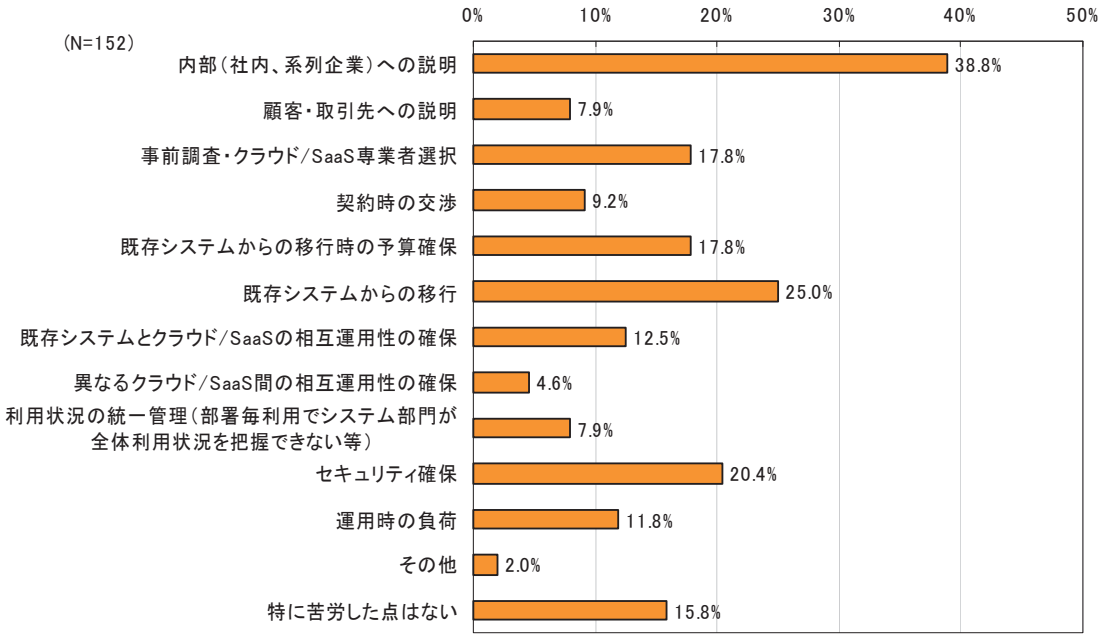
Q7　貴社では、社内のクラウド/SaaS 利用において、クラウド/SaaS 専業者選定や契約等をどのように管理していますか。最も貴社の状況に近いものを 1 つお選び下さい。【問 4 でクラウド/SaaS 専業者を利用していないと回答した方以外】



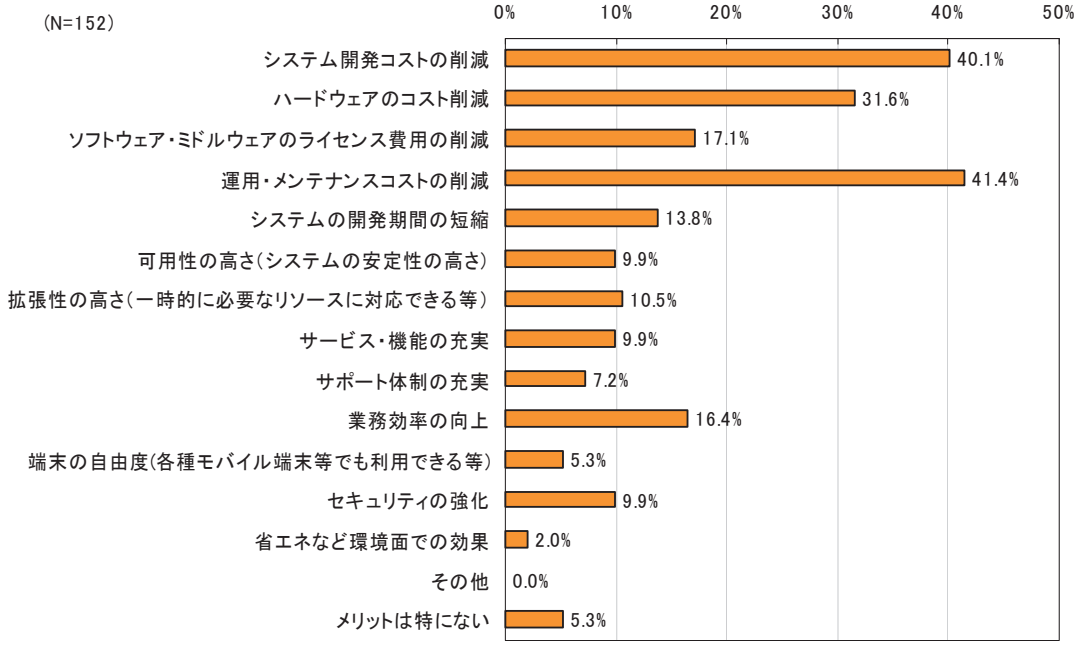
Q8　貴社では、社内のクラウド/SaaS 利用において、アカウント管理や変更管理等の運用面の管理をどのように行っていますか。最も貴社の状況に近いものを 1 つお選び下さい。



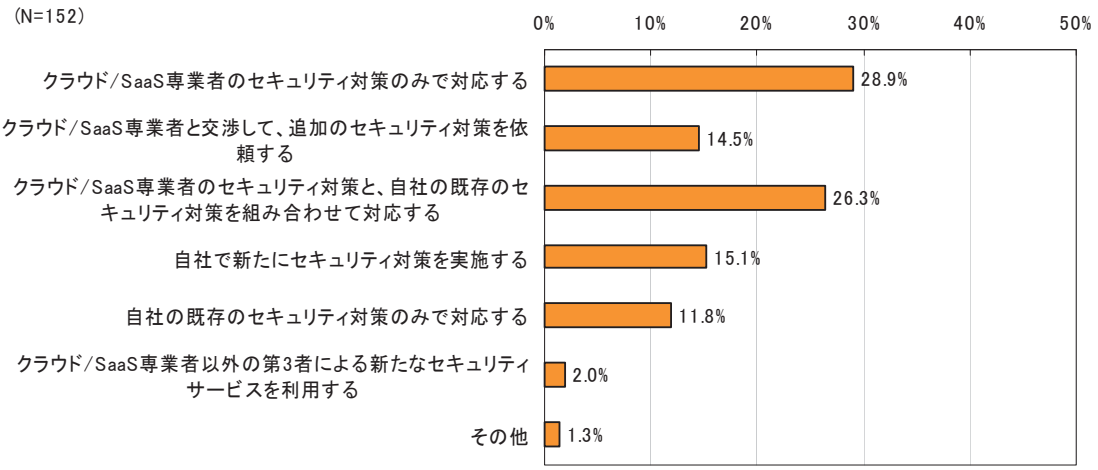
Q9　貴社でクラウド/SaaS を導入するに当たり、苦労したのはどのような点ですか。当てはまるものを 3 つまでお選び下さい。



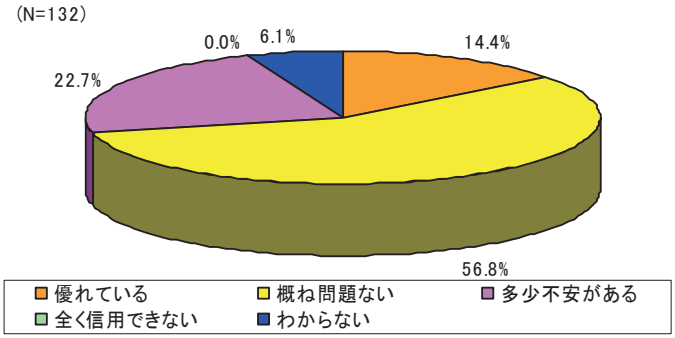
Q10　貴社でクラウド/SaaS を導入したことで、得られたメリットは何ですか。当てはまるものを 3 つまでお選び下さい。



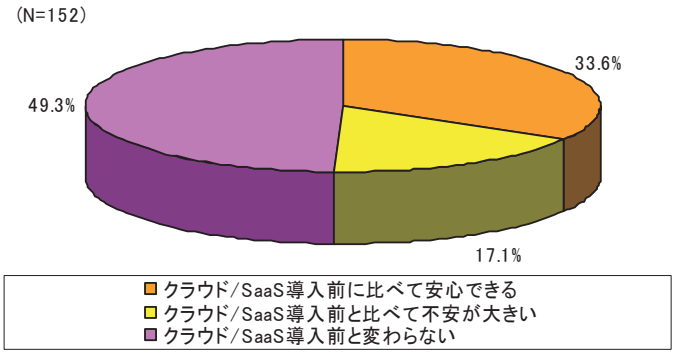
Q11　貴社でクラウド/SaaS を導入する際、どのようなセキュリティ対策の方針をとっていますか。最も貴社の状況に近いもの 1 つお選び下さい。



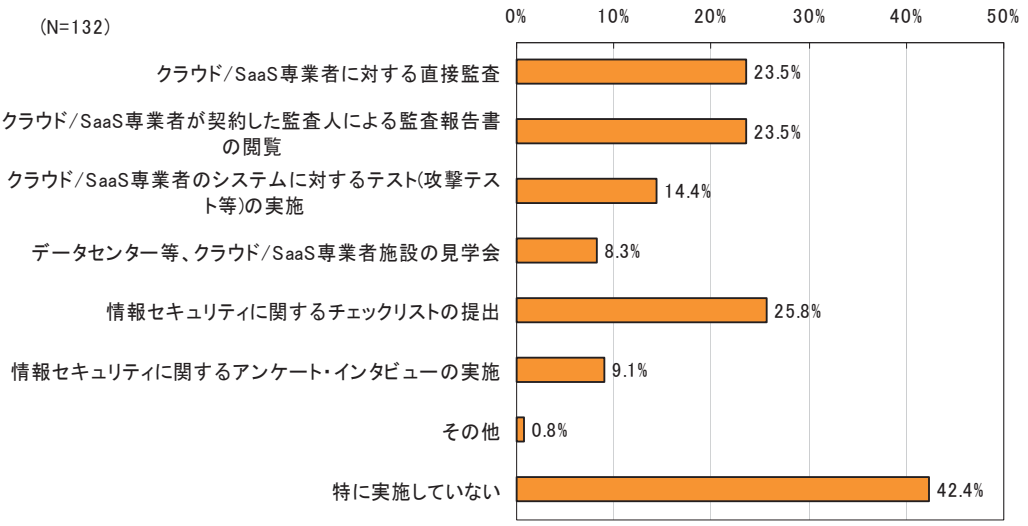
Q12　貴社が利用しているクラウド/SaaS 専業者において実施されているセキュリティ対策のレベルをどのように評価していますか。当てはまるものを 1 つお選び下さい。【問 4 でクラウド/SaaS 専業者を利用していないと回答した方以外】



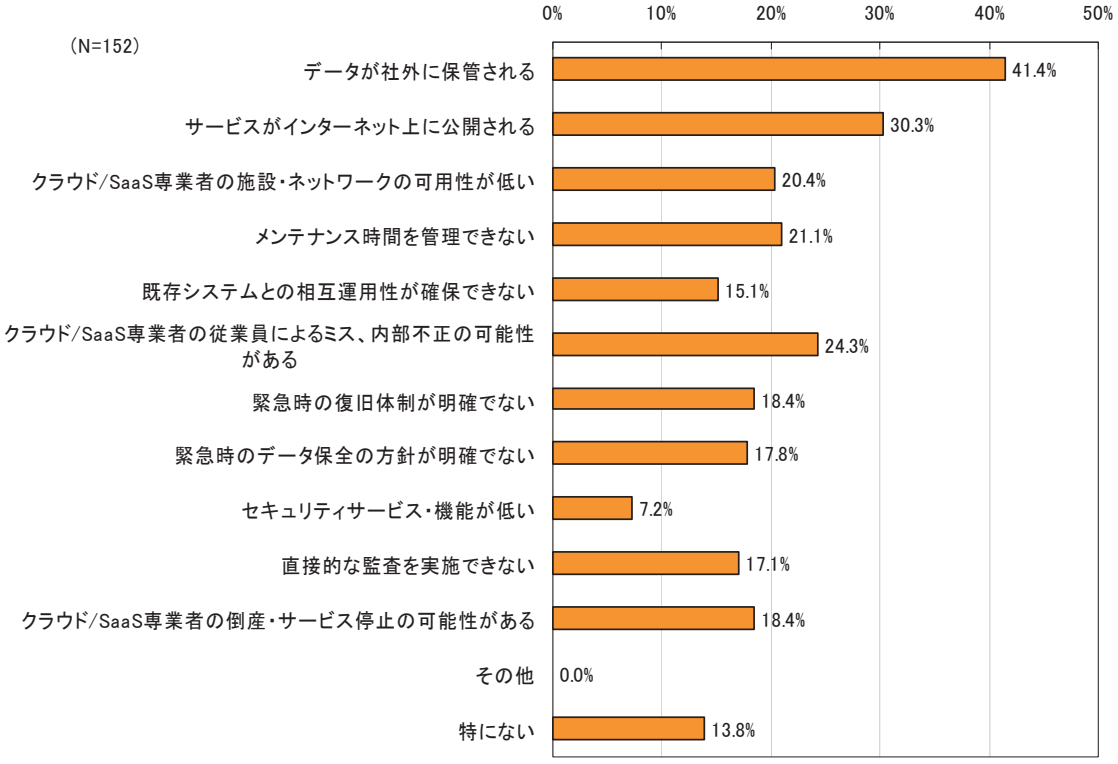
Q13　貴社のクラウド/SaaS 移行前のシステムと比較して、現在利用しているクラウド/SaaS のセキュリティレベルをどのように評価していますか。当てはまるものを 1 つお選び下さい。



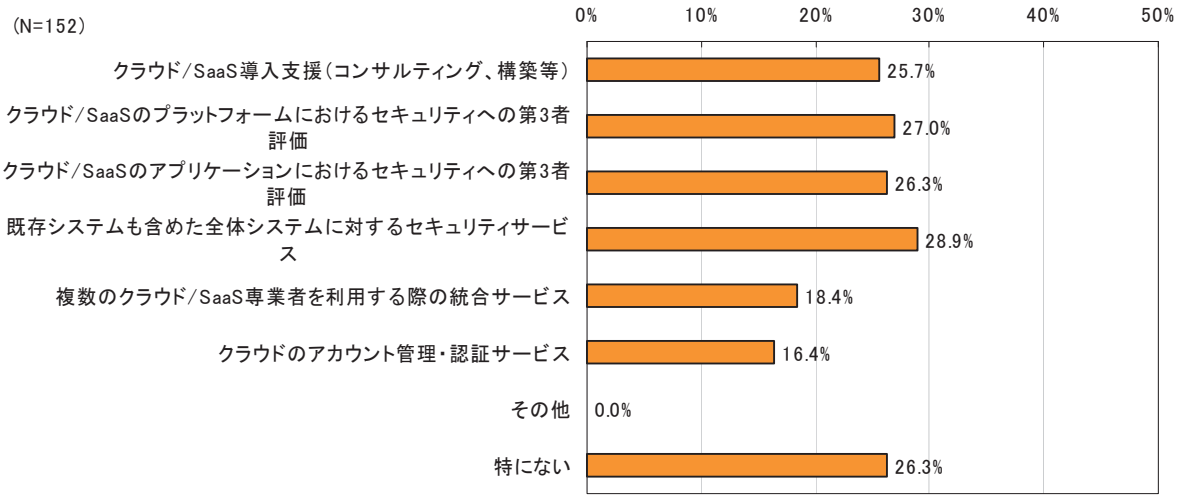
Q14　貴社でクラウド/SaaS 専業者に対して定期的に実施しているセキュリティのチェック体制はありますか。実施しているものを**すべて**お選び下さい。【問 4 でクラウド/SaaS 専業者を利用していないと回答した方以外】



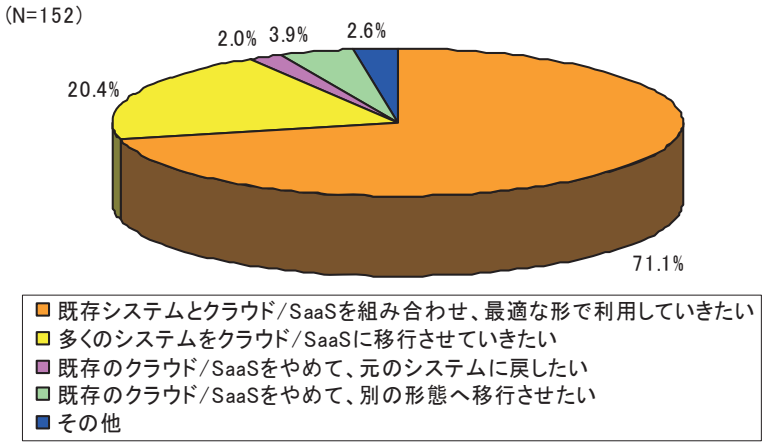
Q15　クラウド/SaaS 利用におけるセキュリティ上の課題はどういった点にあると思いますか。当てはまるものをすべてお選び下さい。



Q16　今後クラウド/SaaS 利用において、どのようなサービスを充実してほしいと思いますか。当てはまるものを**すべて**お選び下さい。



Q17　貴社の情報システム利用における長期的な展望をどのように考えていますか。当てはまるものを 1 つお選び下さい。



アンケート調査票

【第 1 次調査】あなたの勤務先の情報システムに関するアンケート

◇貴社の基本情報についてお伺いいたします。

F1　貴社が属する業種は次のうちどれですか。当てはまるものを 1 つお選び下さい。【必須】

1. 建設業
2. 製造業
3. 電気・ガス・熱供給・水道業
4. 運輸、倉庫業
5. 卸売・小売業、飲食店、宿泊業
6. 金融・保険業
7. 不動産業
8. 電気通信業
9. 情報、IT 関連
10. 出版・放送業
11. 医療・福祉関連業
12. 教育・学習支援業
13. その他サービス業
14. その他

F2　貴社の従業員数は次のうちどれですか。当てはまるものを 1 つお選び下さい。【必須】

1. 20 人以下
2. 21 人～50 人以下
3. 51 人～100 人以下
4. 101～300 人以下
5. 301～1,000 人以下
6. 1,001～5,000 人以下
7. 5,001～10,000 人以下
8. 10,001 人以上

F3　貴社の売上高は次のうちどれですか。当てはまるものを 1 つお選び下さい。【必須】

1. 1 億円未満
2. 1 億～10 億円未満
3. 10 億～100 億円未満
4. 100 億～1,000 億円未満
5. 1,000 億円以上

F4　貴社の直近年度の IT 投資額（予算）について、当てはまるものを 1 つお選び下さい。【必須】

1. 投資なし
2. 500 万円未満
3. 500 万円～1,000 万円未満
4. 1,000 万円～5,000 万円未満
5. 5,000 万円～1 億円未満
6. 1 億円～10 億円未満
7. 10 億円～100 億円未満
8. 100 億円以上
9. わからない

F5　F4 の IT 投資額に対するセキュリティ対策費用額の割合について、当てはまるものを 1 つお選び下さい。【F4 で選択肢 1、9 以外を選択した方】

1. 投資なし
2. 1%未満
3. 1～3%未満
4. 3～5%未満
5. 5～10%未満
6. 10～20%未満
7. 20～30%未満
8. 30%以上
9. わからない

◇ユーザがネットワークを通じてリソースを意識せずに利用できるサービス（クラウド・コンピューティング、SaaS: Software as a Service、ASP: Application Service Provider 等）[19]に関して、貴社の情報システムにおける利用状況についてお伺いいたします。

Q1　貴社の情報システムにおいて上記のようなネットワーク上のサービスを利用していますか。当てはまるものを 1 つお選び下さい。【必須】

1. 利用している
2. 現在利用していないが、今後利用を検討している
3. 現在利用しておらず、今後も利用する予定はない
4. わからない

[19]一般的なデータセンター、ハウジング・ホスティングは除く。

Q2　貴社で上記のようなネットワーク上のサービスを利用していない理由は何ですか。当てはまるものすべてお選び下さい。【Q1 で「3. 現在利用しておらず、今後も利用する予定はない」と回答された方のみ】

1. 必要性がない
2. 内部（社内、系列企業等）の理解を得られなかった
3. 顧客・取引先の理解を得られなかった
4. コストメリットが得られない
5. セキュリティに不安がある
6. 信頼性に不安がある
7. システムを外部に出せない規定があるため
8. システム改修時期でないため
9. その他（自由記述）

Q3　貴社における現在の情報システムの状況について、最も近いものを1つお選び下さい。【必須】

1. 委託開発のシステムを中心に利用している
2. 自社開発のシステムを中心に利用している
3. パッケージ製品を中心に利用している
4. ネットワーク上のサービスを中心に利用している
5. その他（自由記述）

Q4　貴社における以下の各情報セキュリティ製品・サービス（ネットワーク上のサービスに限らず）の導入状況をお答え下さい。【必須】

	導入済み	導入検討中	未導入	わからない
メールフィルタリングツール・サービス	□	□	□	□
シングルサインオン	□	□	□	□
シンクライアント	□	□	□	□
統合 ID 管理ツール	□	□	□	□
データ暗号化ツール（DLP: Data Loss Prevention、電子透かし等も含む）	□	□	□	□
ドキュメント・コンテンツ管理ツール（アクセス制御）	□	□	□	□
データバックアップツール・サービス（社内の情報資産に対するディスク/テープバックアップ）	□	□	□	□
ログ収集・保管・解析、変更管理ツール等	□	□	□	□
ウェブアプリケーションファイアウォール	□	□	□	□

【第 2 次調査】クラウド/ SaaS 利用に関する調査

本アンケートはプレ調査「あなたの勤務先の情報システムに関するアンケート」において、貴社の情報システムでクラウド・コンピューティング、SaaS、ASP を「利用している」もしくは、「現在利用していないが、今後利用を検討している」とお答えいただいた方を対象としております。

それ以外の方はご回答いただけませんので、予めご了承下さい。

貴社におけるクラウド・コンピューティング（以下クラウド）及び SaaS の利用状況についてお伺いいたします。なお、本調査においてクラウド及び SaaS を以下のように定義します。

本アンケート調査におけるクラウド/SaaS の定義

クラウド： クラウド・コンピューティングを指すものとし、サーバ等が提供するサービスを、リソースを意識せずにネットワークを通じて使用できるモデルと定義する。SaaS（Software as a Service）や PaaS（Platform as a Service）等を包含したより広い概念とする。
SaaS （Software as a Service）： ユーザ側のコンピュータがソフトウェアを保有するのではなく、ソフトウェアの機能をサービスプロバイダがネットワークを通じて提供するモデルと定義する。ASP（Application Service Provider）の進化形で、利用者にとってより使い勝手が良く、利用価値が向上したものとする。

※以下の設問においてクラウド/SaaS と表現する場合は、上記で定義したクラウド及び SaaS に加えて ASP も含むものとします。

Q1　貴社の各情報システムに関するクラウド/SaaS の利用（クラウド上に構築しているものも含む）状況をお答え下さい。【必須】

A	基幹系システム	利用中	利用検討中	利用予定なし
1	顧客管理（CRM）	□	□	□
2	営業支援（SFA）	□	□	□
3	販売・在庫管理	□	□	□
4	生産管理	□	□	□
5	企業資源計画（ERP）	□	□	□
6	勤怠管理	□	□	□
7	給与計算	□	□	□
8	会計・財務	□	□	□
9	基幹系システム： その他（自由記述）	□	□	□

B	非基幹系システム	利用中	利用検討中	利用予定なし
1	グループウェア	□	□	□
2	メール（ウェブメール含む）	□	□	□
3	テレビ会議システム	□	□	□
4	SNS、チャットツール	□	□	□
5	文書ツール（Office 系）	□	□	□
6	帳票・文書管理システム	□	□	□
7	e ラーニング	□	□	□
8	ファイル転送ツール	□	□	□
9	ホームページ運営	□	□	□
10	EC サイト運営	□	□	□
11	コールセンター支援	□	□	□
12	ウィルス対策（セキュリティ）	□	□	□
13	侵入検知（セキュリティ）	□	□	□
14	ウィルス対策、侵入検知以外のセキュリティ関連サービス（自由記述）	□	□	□
15	非基幹系システム： その他（自由記述）	□	□	□

Q2　貴社の問 1 のシステムを含む全社の全情報システムにおけるクラウド/SaaS の利用割合はどの程度ですか。当てはまるものを 1 つお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. 5%未満
2. 5～10%未満
3. 10～20%未満
4. 20～30%未満
5. 30～40%未満
6. 40～50%未満
7. 50～60%未満
8. 60～70%未満
9. 70～80%未満
10. 80～90%未満
11. 90～100%

Q3　貴社ではクラウド/SaaS をどのような形態で構築、利用していますか。最も貴社の状況に近いものを 1 つお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】
※　Q1 で A、B 両方において「利用中」と回答した場合はそれぞれについて回答。片方のみ「利用中」と回答した場合は、片方のみ回答。

【A.基幹系システム】
1. 外部のクラウド/SaaS 専業者のクラウド環境を利用している。
2. 自社にクラウド環境を構築している。

【B.非基幹系システム】
1. 外部のクラウド/SaaS 専業者のクラウド環境を利用している。
2. 自社にクラウド環境を構築している。

Q4　貴社ではクラウド/SaaS 専業者（直接クラウド/SaaS のプラットフォームやアプリケーションを提供する事業者とし、導入支援のみを行う事業者等は含まない）を合計何社利用していますか。当てはまるものを 1 つお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】
※　Q1 で A、B 両方において「利用中」と回答した場合はそれぞれについて回答。片方のみ「利用中」と回答した場合は、片方のみ回答。

【A.基幹系システム】
1. 1 事業者のみ
2. 2～5 事業者
3. 6～10 事業者
4. 11 事業者以上
5. 利用していない（自社及び自社グループ内のみで構築、利用している）

【B.非基幹系システム】
1. 1 事業者のみ
2. 2～5 事業者
3. 6～10 事業者
4. 11 事業者以上
5. 利用していない（自社及び自社グループ内のみで構築、利用している）

Q5　貴社でクラウド/SaaS を導入する際、どのように行いましたか。当てはまるものを**すべて**お選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】
※　Q1 で A、B の両方において「利用中」と回答した場合はそれぞれについて回答。片方のみ「利用中」と回答した場合は、片方のみ回答。

【A.基幹系システム】

1. クラウド/SaaS 専業者の導入支援を受けた
2. クラウド/SaaS 専業者以外の事業者による導入支援（コンサルティング、実際のクラウド/SaaS 構築を含む）を受けた
3. 自社で導入した
4. わからない

【B.非基幹系システム】

1. クラウド/SaaS 専業者の導入支援を受けた
2. クラウド/SaaS 専業者以外の事業者による導入支援（コンサルティング、実際のクラウド/SaaS 構築を含む）を受けた
3. 自社で導入した
4. わからない

Q6　貴社でクラウド/SaaS を導入するに当たり、クラウド/SaaS 専業者の利用検討、選定において何を重視しましたか。当てはまるものを 5 つまでお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. 価格
2. 機能・サービスの質
3. 規模
4. 実績（既存顧客、ユーザ数）
5. セキュリティ対策
6. 事業継続性（信頼性）
7. データセンターの場所（国内限定等）
8. サポート体制
9. 認証・認定等の取得
10. 第 3 者の推薦（コンサルティング等による仲介）
11. わからない
12. その他（自由記述）

Q7　貴社では、社内のクラウド/SaaS 利用において、クラウド/SaaS 専業者選定や契約等をどのように管理していますか。最も貴社の状況に近いものを 1 つお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方で、Q4 で選択肢 5 を選択していない場合】

1. 情報システム部門で一括管理している
2. 調達（アウトソーシング担当）部門で一括管理している
3. 各事業部門や部署で個別に管理している
4. 対象システムのオーナーシップに応じてケースバイケース
5. その他の場合（自由記述）

Q8　貴社では、社内のクラウド/SaaS 利用において、アカウント管理や変更管理等の運用面の管理をどのように行っていますか。最も貴社の状況に近いものを 1 つお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. 情報システム部門で一括管理している
2. 調達（アウトソーシング担当）部門で一括管理している
3. 各事業部門や部署で個別に管理している
4. 委託先で管理している
5. 対象システムのオーナーシップに応じてケースバイケース
6. その他の場合（自由記述）

Q9　貴社でクラウド/SaaS を導入するに当たり、苦労したのはどのような点ですか。当てはまるものを 3 つまでお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. 内部（社内、系列企業）への説明
2. 顧客・取引先への説明
3. 事前調査・クラウド/SaaS 専業者選択
4. 契約時の交渉
5. 既存システムからの移行時の予算確保
6. 既存システムからの移行
7. 既存システムとクラウド/SaaS の相互運用性の確保
8. 異なるクラウド/SaaS 間の相互運用性の確保
9. 利用状況の統一管理（部署毎に利用しているため、情報システム部門が全体の利用状況を把握できない等）
10. セキュリティ確保
11. 運用時の負荷
12. その他（自由記述）
13. 特に苦労した点はない

Q10　貴社でクラウド/SaaS を導入したことで、得られたメリットは何ですか。当てはまるものを 3 つまでお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. システム開発コストの削減
2. ハードウェアのコスト削減
3. ソフトウェア・ミドルウェアのライセンス費用の削減
4. 運用・メンテナンスコストの削減
5. システムの開発期間の短縮
6. 可用性の高さ（システムの安定性の高さ）
7. 拡張性の高さ（一時的に必要なリソースに対応できる等）
8. サービス・機能の充実

9. サポート体制の充実
10. 業務効率の向上
11. 端末の自由度(各種モバイル端末等でも利用できる等)
12. セキュリティの強化
13. 省エネなど環境面での効果
14. その他（自由記述）
15. メリットは特にない

Q11　貴社でクラウド/SaaS を導入する際、どのようなセキュリティ対策の方針をとっていますか。最も貴社の状況に近いもの 1 つお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. クラウド/SaaS 専業者のセキュリティ対策のみで対応する
2. クラウド/SaaS 専業者と交渉して、追加のセキュリティ対策を依頼する
3. クラウド/SaaS 専業者のセキュリティ対策と、自社の既存のセキュリティ対策を組み合わせて対応する
4. 自社で新たにセキュリティ対策を実施する
5. 自社の既存のセキュリティ対策のみで対応する
6. クラウド/SaaS 専業者以外の第 3 者による新たなセキュリティサービスを利用する
7. その他（自由記述）

Q12　貴社が利用しているクラウド/SaaS 専業者において実施されているセキュリティ対策のレベルをどのように評価していますか。当てはまるものを 1 つお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方で、Q4 で選択肢 5 を選択していない場合】

1. 優れている
2. 概ね問題ない
3. 多少不安がある
4. 全く信用できない
5. わからない

Q13　貴社のクラウド/SaaS 移行前のシステムと比較して、現在利用しているクラウド/SaaS のセキュリティレベルをどのように評価していますか。当てはまるものを 1 つお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. クラウド/SaaS 導入前に比べて安心できる
2. クラウド/SaaS 導入前と比べて不安が大きい
3. クラウド/SaaS 導入前と変わらない

Q14　貴社でクラウド/SaaS 専業者に対して定期的に実施しているセキュリティのチェック体制はありますか。実施しているものを**すべて**お選び下さい。【Q1 で「利用中」を 1 つ以上選択した方で、Q4 で選択肢 5 を選択していない場合】

1. クラウド/SaaS 専業者に対する直接監査
2. クラウド/SaaS 専業者が契約した監査人による監査報告書の閲覧
3. クラウド/SaaS 専業者のシステムに対するテスト(攻撃テスト等)の実施
4. データセンター等、クラウド/SaaS 専業者施設の見学会
5. 情報セキュリティに関するチェックリストの提出
6. 情報セキュリティに関するアンケート・インタビューの実施
7. その他（自由記述）
8. 特に実施していない

Q15　クラウド/SaaS 利用におけるセキュリティ上の課題はどういった点にあると思いますか。当てはまるものをすべてお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. データが社外に保管される
2. サービスがインターネット上に公開される
3. クラウド/SaaS 専業者の施設・ネットワークの可用性が低い
4. メンテナンス時間を管理できない
5. 既存システムとの相互運用性が確保できない
6. クラウド/SaaS 専業者の従業員によるミス、内部不正の可能性がある
7. 緊急時の復旧体制が明確でない
8. 緊急時のデータ保全の方針が明確でない
9. セキュリティサービス・機能が低い
10. 直接的な監査を実施できない
11. クラウド/SaaS 専業者の倒産・サービス停止の可能性がある
12. その他（自由記述）
13. 特にない

Q16　今後クラウド/SaaS 利用において、どのようなサービスを充実してほしいと思いますか。当てはまるものを**すべて**お選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. クラウド/SaaS 導入支援（コンサルティング、構築等）
2. クラウド/SaaS のプラットフォームにおけるセキュリティへの第 3 者評価
3. クラウド/SaaS のアプリケーションにおけるセキュリティへの第 3 者評価
4. 既存システムも含めた全体システムに対するセキュリティサービス
5. 複数のクラウド/SaaS 専業者を利用する際の統合サービス
6. クラウドのアカウント管理・認証サービス

7. その他（自由記述）
8. 特にない

Q17　貴社の情報システム利用における長期的な展望をどのように考えていますか。当てはまるものを 1 つお選び下さい。【Q1 で「利用中」を 1 つ以上選択した方】

1. 既存システムとクラウド/SaaS を組み合わせ、最適な形で利用していきたい
2. 多くのシステムをクラウド/SaaS に移行させていきたい
3. 既存のクラウド/SaaS をやめて、元のシステムに戻したい
4. 既存のクラウド/SaaS をやめて、別の形態へ移行させたい
5. その他（自由記述）

セキュリティ市場・技術調査報告書

発　行　日　　平成22年３月
編集・発行　　社団法人　電子情報技術産業協会
　　インダストリ・システム部
　　企画グループ
　　〒100-0004　東京都千代田区大手町1-1-3
　　大手センタービル
　　TEL　(03)5218-1057
印　　刷　　三 協 印 刷 株 式 会 社