SaaS（Software as a Service）と情報セキュリティ

前　川　　徹
サイバー大学 IT 総合学部・教授

要　旨

ソフトウェアの機能をネットワーク経由で提供する SaaS が普及しつつある。初期コストのみならず，運用コストの削減が期待できる SaaS はユーザーにとってメリットが大きい。既存のアンケート調査によれば，ユーザーは SaaS ベンダーからの情報漏えいやネットワーク障害などによるサービス中断を恐れている。しかし一方で，信頼できる SaaS ベンダーであれば，SaaS を利用した方が，高いセキュリティと信頼性を得られると考えるユーザーも少なくない。この傾向は，SaaS をよく理解しているユーザーほど高くなる。こうしたことを考えると，SaaS に対する理解が深まるとともに，SaaS の利用に伴う情報セキュリティに関する不安は小さくなり，逆に情報セキュリティを高める一つの方法として SaaS を利用するユーザーが増加する可能性がある。

キーワード：SaaS, Software as a Service, 情報セキュリティ

第 1 章　はじめに

第 1 節　SaaS とは何か

SaaS とは，Software as a Service の略で，直訳すれば「サービスとしてのソフトウェア」であり，「従来，ソフトウェアが提供していた機能を，ネットワークを通じてサービスとして提供（販売）する仕組み」である。通常，SaaS のユーザーは，ネットワークとしてインターネットを利用し，ウェブ・ブラウザを用いてそのソフトウェアを利用する。

SaaS をユーザー側からみれば，ソフトウェアを所有するのではなく，ネットワークを介して利用することを意味する。この仕組みは電力に例えると理解が容易である。つまり，発電所を社内に設置して電力を利用するのではなく，電力会社の発電所で発電された電力をコンセントから必要に応じて利用する形態である。一言でいえば，情報システムを「所有から利用」に転換するものだと位置づけられる。

原稿受付日：2008 年 12 月 2 日
原稿受理日：2009 年 2 月 13 日

一方，SaaS をベンダー側からみると，「ドリルを販売するビジネスモデル」ではなく「壁に穴をあけるサービスを提供するモデル」だと表現することができる。Theodore Levitt が『マーケティング発想法』に「顧客は 4 分の 1 インチのドリルが欲しいわけではない。4 分の 1 インチの穴が欲しいのだ」と書いたように，ユーザーが必要としているのは情報システムそのものではなく，その情報システムが提供する情報処理機能（能力）である。この考えに基づき，ソフトウェア製品や情報システムを販売するのではなく，情報処理機能（能力）をネットワーク経由でユーザーに直接提供するサービスが SaaS だということになる。

第 2 節　マルチ・テナントとシングル・テナント

SaaS を，ユーザーが必要とするシステム機能を，ネットワークを通じて提供するサービスとして定義すると，従来から存在している ASP（Application Service Provider）との差がまったくないことになる。SaaS の定義については，2008 年秋の時点において，コンセンサスが得られたものはなく，ASP と SaaS の関係ははっきりしない。ここでは SaaS は ASP に含まれるものだとして扱う。

ただし，この数年，注目を浴びている主な SaaS には以下のような共通的な特徴がある。

⑴　マルチ・テナント方式である
⑵　ソースコードを改変せずにカスタマイズが可能である
⑶　当初から SaaS として設計されている

これらの特徴は相互に関連があるが，もっとも重要な特徴が，一つのシステムで複数のユーザーに対応できるというマルチ・テナント方式というアーキテクチャである。

従来の ASP は，ユーザーごとに論理的に独立した情報システム（インスタンス）を割り当ててサービスを提供する形態（シングル・テナント方式）が多かった。シングル・テナント方式の場合，それぞれのユーザーに応じてソースコードを改変することによって，ユーザーインタフェースはもちろん，提供する機能，情報処理のフローなどを自由に変更できる。しかし，その反面，ユーザー数が増加すれば，それだけ管理するソフトのバージョンの数が多くなり，管理コストの増加を招くという短所があった。例えば，個々にカスタマイズされている場合，そのアプリケーションソフトのバージョンアップは非常に手間のかかる作業になる。

しかし，マルチ・テナント方式であれば，1 つのインスタンスで複数のユーザーにサービスを提供するため，管理コストを大幅に削減できると同時に，利用者全員に同時に最新バージョンの機能を提供できる。

マルチ・テナント方式であることは，同時にソースコードを改変することなくカスタマイズが可能であることを意味する。多くの SaaS では，メタデータを用いてカスタマイズが可能になっており，個々のサービスによって，そのカスタマイズ可能な範囲は異なるも

のの，一般的にはユーザーインタフェースや項目名はもちろん，レポートの様式から業務フローまで自由に設計できる。また，メタデータでのカスタマイズでは対応できない場合には，公開されている API を利用し，追加的にアプリケーションを作成が可能である。

こうした条件を満たすために SaaS は，その設計・開発時から多様なカスタマイズがメタデータによって自由にできるように配慮されている。つまり多くの SaaS は，当初から SaaS として設計されているのである。

もちろん，既存のソフトウェアを SaaS 向けに修正することは不可能ではないが，かなり大幅な修正が必要になると考えられる。また，当然のことながら，SaaS の場合，利用者側はブラウザを通して利用することになるため，ウェブ・アプリケーションとして設計，提供される。これによって，利用者に必要なソフトウェアは標準的なブラウザ・ソフトだけになり，導入（利用）が非常に簡単になる。

さらに，多くの SaaS は他のアプリケーションとの連携を前提として設計されている。これは，利用企業が必要とする情報処理機能をすべて統合的にサービスするのではなく，複数の SaaS を連携して利用する，あるいは既存の業務アプリケーションと連携して利用することを想定して提供されているからである。

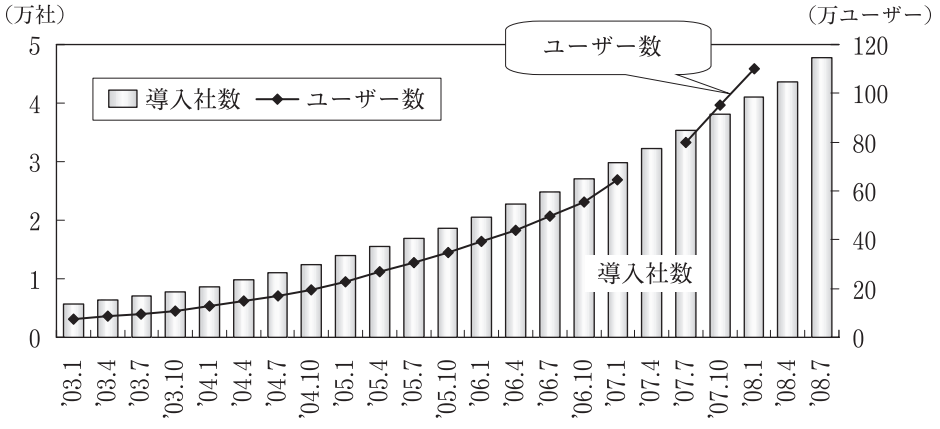
第 2 章　SaaS の事例

次に，SaaS の事例をいくつか紹介する。

第 1 節　事例 1：Salesforce

Salesforce は，1999 年にオラクルで役員の経験をもつ Marc Benioff が創業した Salesforce.com が 2000 年 4 月からサービスを提供している顧客管理および営業支援のための SaaS 型の CRM/SFA ソリューションである。

Salesforce の利用者数は，2009 年 1 月末現在，全世界で 55,400 社，アカウント数は 2009 年 1 月末時点で 150 万以上に達している（図 1 参照）。



（出典）　Salesforce.com（http://www.salesforce.com/company/investor/financials/）

図 1　Salesforce.com の利用社数・ユーザー数

Salesforce.com の売上高は，2004 年 1 月期の 9,600 万ドルであったが，2009 年 1 月期には 10 億 7,700 万ドルと，5 年間で 11 倍以上になっている。

Salesforce の特徴は，部門や役割ごとの異なるニーズに応じてユーザーごとに Salesforce を柔軟にカスタマイズできること，他システムとの連携，新規アプリケーションの作成を実現するオンデマンド・プラットフォーム「force.com」を提供していること，導入支援やトレーニングなどを行うサポートサービス「Successforce」を提供していることにある。

また，Salesforce は随時アップデートされ，提供されているのは常に最新のバージョンであるが，カスタマイズ情報はメタデータとしてユーザーごとに管理されており，互換性を気にすることなく常に最新の機能が利用できる。Salesforce.com 側からみれば，すべての利用者に同じバージョンでサービスを提供するため，運用管理コストを低減することができる。ちなみに，この 7 年間で 22 回のバージョンアップが実施されている。

第 2 節　事例 2：ネット de 会計（ネット de 記帳）

「ネット de 会計」は 2000 年 3 月に設立されたビジネスオンライン株式会社が，2000 年 8 月からサービスを始めた SaaS であり，商工会向けには「ネット de 記帳」として全国 34 都道府県の約 9 万会員以上に利用されている。

ネット de 会計は，インターネットで帳簿入力や月次決算，期末決算が可能な中小企業向けの会計システムであり，システムやデータがビジネスオンライン社あるいは商工会連合会のサーバーで管理されているため，利用者はソフトウェアのインストールやアップデート，データのバックアップなどの作業をしなくてもよい。

また，必要に応じて，商工会や会計事務所とリアルタイムで情報を共有することができるため，日々の仕訳取引会計は自社で行い，分析や決算は会計事務所に依頼するとか，記帳が正しいかのチェックを会計事務所や商工会に相談することも可能である。このため，ネット de 会計には「付箋機能」があり，確認が必要な伝票データに付箋を貼ることによって，会計事務所や商工会とのコミュニケーションをスムーズにすることができる。これは，ネットの向こう側にアプリケーションソフトとデータがあることによって生まれる長所である。

第 3 節　事例 3：Google Docs

Google Docs は，Google の Web ベース表計算「Google Spreadsheet」と 2003 年 6 月に Google が買収した Web ベースのワードプロセッサ「Writely」を合体させたもので，2006 年 10 月にベータ版が公開され，現在はプレゼンテーション機能も追加されている。

ネットに接続したパソコンと標準的なブラウザがあればワープロ，表計算，プレゼンテーションソフトが利用できる。ユーザー登録をすれば，利用は無料である。ワープロは MS Word ファイルや ODF ファイル（OpenOffice.org で利用されているファイル）にダウン

ロードでき，表計算はCSV形式でダウンロードできるので，パソコン側に取り込んでオフラインで編集することも可能である。

最大の特徴は，ネット上でのファイル共有が可能な点にあり，ユーザー毎に「閲覧のみ」，「編集」可能の選択ができる。この機能を利用すれば，複数の利用者が地理的に離れた場所で共同してドキュメントを作成することができる。

ちなみに，作成した文書，表をウェブ上で公開することも可能である。

第3章　SaaSのメリット・デメリット

第1節　利用者側からみたメリット

まず，利用者（利用企業）側からみたSaaSのメリット・デメリットを考えてみる。

一般的に，SaaSは，自前で情報システムを構築するよりコストが少なくて済むと言われている。しかし，これは導入コストであって，情報システムの導入から廃棄に渡るライフ・サイクル・コストではない。利用企業の規模，利用するSaaSの料金体系，比較対象となるパッケージソフトあるいは受託開発するソフトウェア，利用期間などの条件によって比較結果は変わりうる。後述するように，SaaSは保守運用のプロセスにおいて規模の経済が働くため，理論的にはSaaSの方が安くなるはずなのだが，現実には，逆にSaaSの方が高くなるケースもあると思われる。

ただ，少なくとも，導入に要する初期コストはSaaSの方が安い。自社内に情報システムを構築する場合には（それがパッケージソフトを利用する場合であっても），ある程度の投資が必要になるが，SaaSの場合にはインターネットの接続されたパソコンと一般的なブラウザ・ソフトがあれば，SaaSを利用できるからである。

また，利用ユーザー数（ライセンス数）や利用する機能などによって決まる料金体系を採用しているサービスが多いため，試験的に必要な機能だけ導入し，自社の業務に合っていなければ解約することも可能であるため，リスクも小さい。自社で情報システムを構築した場合，設計・開発工程に投じたコストはサンクコストとなり，仮にその情報システムが不要になった場合，そのコストは回収できない。一方，SaaSの場合には，社内の一部で試験的に利用を始め，効果があれば段階的に利用を拡大していくという柔軟な導入が可能である。

導入までの期間が短いのもSaaSの大きなメリットである。新規に情報システムを開発する場合はもちろん，パッケージソフトを利用する場合に比べても，導入に要する時間は短くてすむ。SaaSを利用する場合でも，既存のアプリケーションとの連携やカスタマイズのためにある程度の期間が必要なケースもあるが，それでも社内でシステム構築する場合に比べれば，短い期間で導入することが可能である。

また，SaaSを利用することによって，IT関連資産を小さくでき，ROA（総資産利益率）の向上をはかることができる。特にIT資産は直接的に売上げにつながる資産ではなく，また帳簿上の償却より実際の価値の方が早く低下する資産であるため，SaaSの利用

は資本効率を考えた場合には有利である。

第 2 節　利用者側からみたデメリット

一方，SaaS を利用するデメリットとして，システムがサービスを提供するベンダーにあり，また通常はインターネットを経由して利用するため，そのサービスの可用性を利用企業側では完全にコントロールできないという問題がある。この問題を根本的に解決することはできないが，SaaS ベンダー及び ISP と SLA[(1)] を結ぶことによって，リスクを移転することは可能である[(2)]。

また，SaaS は一般的にマルチ・テナント方式で提供されるため，そのカスタマイズには限界がある。メタデータを利用して自由にカスタマイズできると述べたが，自社で情報システムを持つ場合に比べればカスタマイズ可能な範囲は狭くなる。しかし，パッケージソフトを利用する場合を考えれば，大幅なカスタマイズの実施によって，その後のバージョンアップに対応できなくなるといったケースもあるので，そもそも自社のビジネスプロセスに合わせて際限なくカスタマイズを行うという方針は推奨されるものではない。つまり，パッケージソフトを利用する場合でも，SaaS を利用する場合でも，カスタマイズは一定の範囲に止め，できるだけ業務プロセスをパッケージソフトや SaaS の機能に合わせて変更するという発想が必要になる。

さらに，従来型の ASP の場合，アプリケーション間での連携が難しかったこともあり，SaaS についてもアプリケーション間連携が困難であるという誤解が一部にあるが，SaaS の多くは SOA の考え方に従って開発されており，アプリケーション連携のための API が公開されているので，他のアプリケーションとの連携も従来に比べればかなり容易になっている。

第 3 節　ベンダーからみたメリット

ベンダーにとっての最大のメリットは，保守コストの大幅な削減である。利用企業の環境やニーズに合わせて構築，カスタマイズされているシステムをそれぞれのサイトで個別にメンテナンスするより，ベンダー側のサイトの環境で 1 つの情報システムを保守できる SaaS の方が，メンテナンスコストを大幅に小さくできることは自明である。分かりやすく言えば，100 社のシステムをそれぞれ異なる場所で保守運用するよりは，一カ所でまとめて面倒を見た方がコストがかからないということである。

経済学的に言えば，SaaS は，運用保守のプロセスにおいて供給側の規模の経済が働くビジネスだということである。

ただし，一つの実装された情報システム（インスタンス）で複数の利用企業にサービスを提供するためには，カスタマイズをメタデータで実現するなどの方法によって，マルチ・テナントを実現する必要がある。そのため，単独の利用企業向けの情報システムに比べて，マルチ・テナント方式の SaaS の初期開発費用は多くなるだろう。しかし，マルチ・テナント方式であることは運用保守のプロセスにおいて規模の経済を実現するためには必須で

あり，マルチ・テナントでなければ競合する他社の SaaS との競争に勝つことは難しいと考えられる。

また，SaaS はユーザー数に応じた毎月の料金だけで利用を開始できるため，従来は顧客になり得なかった小規模な企業を顧客として取り込むことができ，市場の裾野を大きく拡大できる。企業が情報システムに充てられる金額は，おおむね企業の規模に比例する。日本の企業の規模別分布は，（他の資本主義経済の国と同じように）大規模な企業は少なく，規模が小さくなるにつれ，その数は多くなる。つまり，情報システムの市場はロングテール市場になっている。供給側の規模の経済が働く SaaS は，従来の情報システムよりコストが小さくなるので，利用企業が負担する料金も自社内に情報システムを構築・維持するより安くなると考えられる。したがって，SaaS は，従来の情報システムのベンダーが標的とすることができなかったロングテール市場を開拓することが可能になる。

さらに，一度 SaaS の利用を始めた企業についてはロックイン効果が働くため，継続的な利用が期待できる。ロックイン効果は通常の情報システムでも発生するが，SaaS の場合には，ユーザーインタフェースに特徴のあるものが多く，アプリケーションとの連携やカスタマイズによってより高いロックイン効果が発生する可能性がある。

第 4 節　ベンダーからみたデメリット

一方，SaaS ベンダーは，安定的にサービスを提供する責任を負うことになる。特に，顧客との間で安定的なサービスを保証する SLA を結んでいる場合には，想定以上の障害が発生した場合，賠償金を支払うというリスクを負うことになる。

また，利用企業のデータを預かる形になるため，情報漏えいのリスクも負う。ただし，データセンターでまとめて管理できることを考えれば，利用企業のそれぞれのサイトで情報セキュリティ対策を高じるよりは効率的に実施可能である。

さらに，SaaS の場合，ベンダーは初期にある程度のまとまった投資をする必要がある。前述のとおり，SaaS の場合には，マルチ・テナント方式にするため，特定の企業向けに同じような情報システムを開発するよりも，開発コストがかかる。これもデメリットの一つとして考える必要がある。

第 4 章　SaaS と情報セキュリティ

第 3 章の第 1 節の「利用者側からみたメリット・デメリット」で述べたように，利用者側からみた SaaS の最大の問題点は，利用するソフトウェアとデータがネットワークの向こう側にあるため，Confidentiality（機密性），Integrity（完全性），Availability（可用性）を自分でコントロールできない点にある。

たとえば，利用者側の努力によって，データの盗難や，改ざんのリスクを直接コントロールすることはできない。また，SaaS ベンダー側のシステムの不具合やネットワーク・トラブルによってサービスが利用できなく可能性があるが，それは利用者からはほとんど何

の技術的対策を講じることができない。もちろん，ネットワークを二重化する，信頼性の高いネットワークを利用するといった対策や，SaaS ベンダーと SLA（サービス・レベル・アグリーメント）を結ぶという間接的な対策はできる。これも重要なことであるが，それでも社内に情報システムがある場合に比べて可用性のコントロールは難しい。

2007 年春に日経 BP 社が日経コミュニケーションの読者に対して行った SaaS に関するアンケートをみても，「社外にデータをあずけるためにセキュリティが問題だ」という回答者の割合は 74.4%もあるし，「ネットワークが止まると使えない」ことをデメリットして挙げた回答者は 61.0%であった（図 2 参照）。

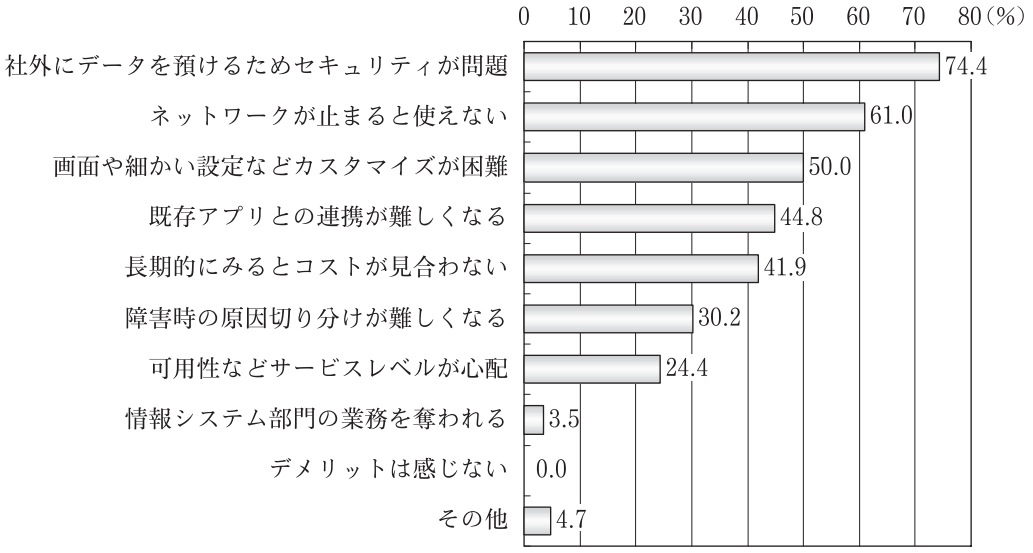
同様の結果は，今年 1 月に（社）コンピュータソフトウェア協会（CSAJ）が実施した，中小企業の経営者と従業員および自営業を対象としたウェブアンケート調査[(3)]にも見ることができる（図 3 参照）。

たとえば，SaaS を利用するデメリットを尋ねたところ，「情報漏えいが心配」が 65.1%で最も多く，次いで「ネットワーク障害があれると使えなくなる」（62.1%）が 2 番となっている。

また，この調査の別の設問で「ネットワーク（インターネット）のトラブルでサービスが中断されることが心配である」という質問に対して「そう思う」あるいは「ややそう思う」と回答した人の割合は 89.3%であり，「SaaS ベンダー側のシステムの不具合によるサービス中断が心配である」は 86.6%となっている。

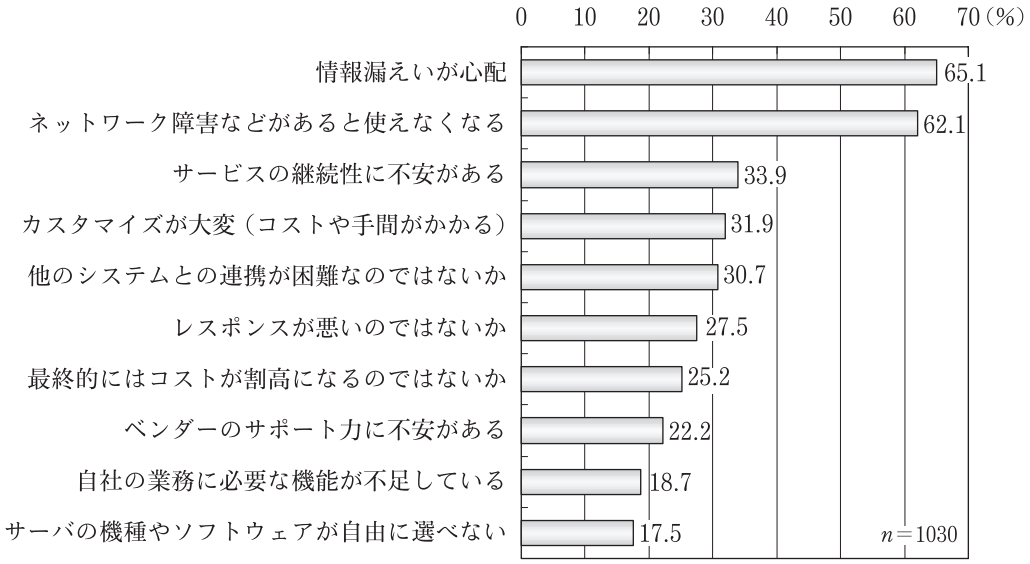
さらに，約 80%の人が，「データセンターへの不正アクセスによる情報漏えいが心配である」や「SaaS ベンダーの社員による情報漏えいが心配である」に「そう思う」あるいは「ややそう思う」と回答している。

しかし，一方で SaaS の方が情報セキュリティ上好ましいという回答もある。先に引用した日経 BP 社のアンケートでも，社外のデータセンターに業務データを置くことについ



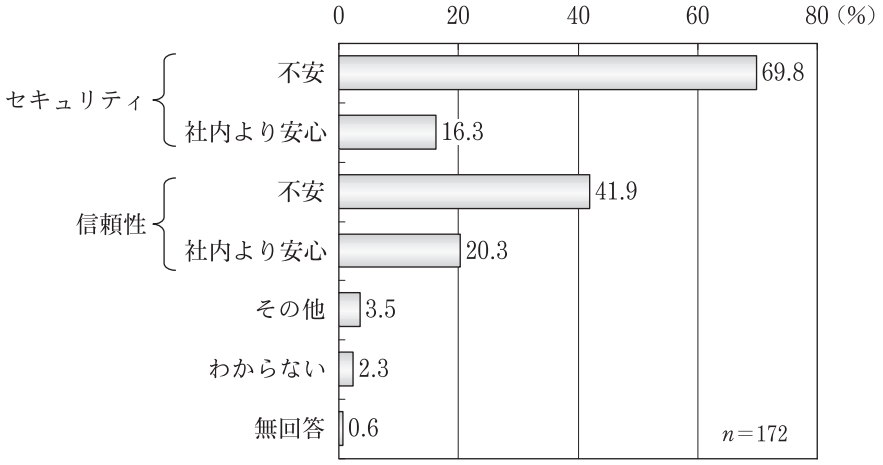
（出典） 日経 ITPro（http://itpro.nikkeibp.co.jp/article/COLUMN/20070606/273780/）

図 2　SaaS のデメリット（日経 BP 社のアンケート）



（出典） コンピュータソフトウェア協会（http://www.csaj.jp/release/08/20080331.pdf）

図 3　SaaS のデメリット（CSAJ）



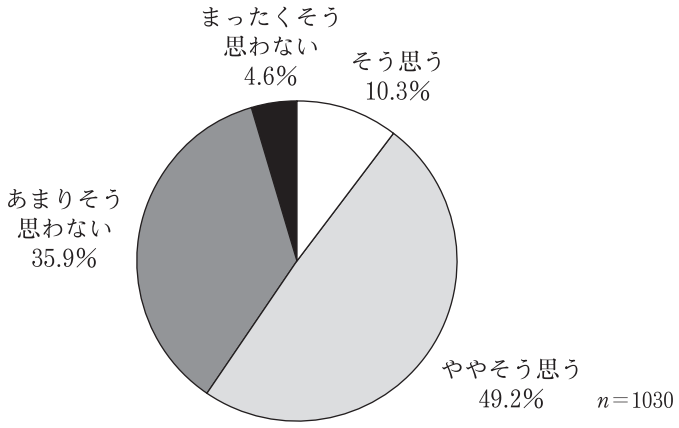
（出典） 日経 ITPro（http://itpro.nikkeibp.co.jp/article/COLUMN/20070606/273780/）

図 4　業務データを社外のデータセンターに置くことについて

て，69.8%に回答者がセキュリティ面で不安であると答えているが，16.3%は社内に置くより安心だと答えている。また，信頼性についても，社外にデータを置くことについて41.9%が不安だと答えているが，20.3%は社内に置くより安心だと答えている（図 4）。

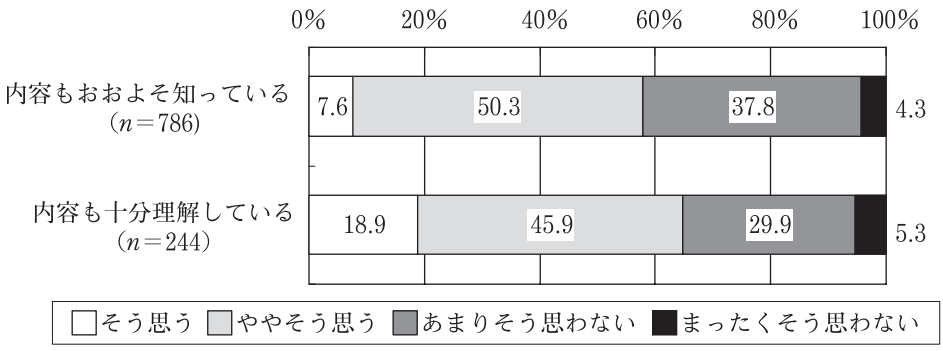
同様に，CSAJ のウェブアンケートでも，「信頼できるベンダーであれば，自社でデータを持つより SaaS を利用した方が情報セキュリティ面で安心である」という質問に対しては，「そう思う」が 10%，「ややそう思う」が 49.2%と回答しており，合計すると約 6 割の人が，信頼できる SaaS ベンダーであれば，自社の情報システムでデータを管理するより SaaS を利用した方が安心だと答えている（図 5 参照）。

この CSAJ のアンケートは，SaaS について，その名称だけでなく「内容も十分に理解している人」と「内容もおおよそ知っている人」を対象にした調査であるが，この「信頼



（出典） コンピュータソフトウェア協会（http://www.csaj.jp/release/08/20080331.pdf）

図 5　信頼できるベンダーの場合の安心感(1)



（出典） コンピュータソフトウェア協会（http://www.csaj.jp/release/08/20080331.pdf）

図 6　信頼できるベンダーの場合の安心感(2)

できるベンダーであれば，自社でデータを持つより SaaS を利用した方が情報セキュリティ面で安心である」という質問に対する回答を認知度別にみると面白いことがわかる。

「内容も十分に理解している」人の方が，信頼できる SaaS ベンダーに任せたほうが安心だという割合が増加するのである。「そう思う」と「ややそう思う」の合計でみると，「内容もおおよそ知っている」人は 57.9%であるが，「内容も十分に理解している」人だと 64.8%となる。特に「そう思う」という割合は，SaaS について「内容もおおよそ知っている」人だと 7.6%であるが，「内容も十分知っている」人だと 18.9%に増加する（図 6 参照）。

こうしたことを考えると，SaaS ベンダーは十分なセキュリティ対策を講じ，利用者の信頼を得る努力をすれば，情報セキュリティ問題はむしろ SaaS にとってプラスに働く要素になる可能性が高いことがわかる。

実際，主要 SaaS ベンダーの多くは，情報セキュリティマネジメントに関する認証であ

るISMSや内部統制に関する監査認定であるSAS 70タイプⅡを取得している。こうした管理面での対策に加えて技術面での対策の強化が，SaaSベンダーの重要な課題になると思われる。

特に，SaaSはインターネットを通して提供されるWebアプリケーションであるために，グローバルな脅威にさらされている。IPAとJPCERT/CCは，2004年7月からソフトウェア等の脆弱性関連情報に関する届出制度（経済産業省告示）に基づいて，ソフトウェア等の脆弱性情報の届出受付を行っているが，制度開始から2008年9月までにウェブアプリケーションの脆弱性に関して2084件の届出を受け付けている(4)。こうした現実を踏まえ，既知の脆弱性に対する対策はもちろん，新しい攻撃方法に対しても迅速に対策を講じていることがSaaS普及の鍵になると思われる。

第5章　SaaS市場の将来

米国の大手金融サービス企業Credit Suisseの予測によれば，SaaSの市場規模は，2007年時点の44億5,500万ドルから5年後の2011年には207億8,900万ドルに拡大する。つまり，SaaS市場は，今後5年間は年平均36%で拡大するとみられている(5)。

SaaSが利用されている領域（業務分野と対象企業）をみると，現状では，業務分野では情報化が比較的最近に始まった領域であるか，対象企業が中小企業であるケースが多い。

たとえば，情報化の歴史が浅いCRM（Customer Relationship Management）やSFA（Sales Force Automation）などの分野では比較的企業の大小を問わずSaaSの利用事例が多い。Salesforce.comを利用している企業は中堅，中小企業が多いが，みずほ銀行のような大企業での利用も進んでいる。

一方，経理や財務会計業務などのように古くから情報化が進んでいる分野の場合には，ほとんどが，小規模な企業での利用である。

つまり現時点では，SaaSが利用されているのは「比較的情報化が最近始まった分野」であるか「対象企業の規模が小さい」領域である。しかし，今後は，比較的規模の大きい企業の財務会計や販売在庫管理のような古くから情報化が行われている分野でSaaS利用が進むのではないかと思われる。

もちろん，巨大企業の基幹システムがSaaS化されるとは考えにくいが，SaaSの適用領域は着実に拡大し，従来型のソフトウェア・ビジネスの領域を浸食していく可能性が高いと考えられる。

第6章　ま　と　め

SaaSの本質は，マルチ・テナントであることによって，運用・保守の工程でも規模の経済が働くことにある。

全プロセスで規模の経済が働くSaaSは，コスト面で従来の情報システムに対して優位

であると考えられる。また，運用コストを削減できる SaaS はユーザーにとってもメリットが大きい。

そのユーザーの最大の関心事は SaaS の情報セキュリティである。特に SaaS ベンダーからの情報漏えい，ネットワーク障害や SaaS ベンダー側のシステム障害によるサービス中断を心配する人が多い。しかし，一方で，信頼できる SaaS ベンダーであれば，SaaS を利用した方が，高いセキュリティと信頼性を得られるという声も少なくない。

こうしたことを考えると，SaaS に対する理解が深まるとともに，SaaS の利用に伴う情報セキュリティに関する不安は小さくなり，逆に情報セキュリティを高める一つの方法として SaaS を利用するユーザーが増加する可能性がある。

このためには，SaaS ベンダーは顧客の信頼に応えられる万全のセキュリティ対策を取る必要がある。

注および引用文献

（1） SLA（Service Level Agreement）とは，利用者にサービスの品質を保証する契約のことで，サービスの稼働率や故障があった場合の最大復旧時間，約束が守れなかった場合のペナルティ（違約金）などを取り決めたもの。

（2） 一般にリスクへの対応は，制御（control），回避（avoidance），移転（transfer），受容（acceptance）に分けられる。

（3） この調査は，ウェブアンケートで実施され，事前調査によって⑴従業員 300 人以下の企業の従業員か経営者あるいは自営業者であって，⑵情報システムの導入に関与しているか関心が高く，かつ⑶SaaS についてある程度以上の知識がある人のみを調査対象としている。詳細は CSAJ のニュースリリース（参考文献の 2）を参照。

（4） 独立行政法人 情報処理推進機構 セキュリティセンター「ソフトウエア等の脆弱性関連情報に関する届出状況」2008 年 10 月 14 日（http://www.ipa.go.jp/security/vuln/report/vuln2008q3.html）を参照。

（5） 出典は，Jason Maynard “The Revolution in Business Software” Apr.2007,（SIIA Software Strategy Summit におけるプレゼンテーション資料）

参考文献

1. 小野亮「失敗しない SaaS 導入の心得　第 2 回　ユーザー・アンケートで見えた，根強い『セキュリティ面の不安』」（http://itpro.nikkeibp.co.jp/article/COLUMN/20070606/273780/）（2008.11.17 確認）
2. （社）コンピュータソフトウェア協会「中小企業における SaaS の利用意向等に関する調査を実施 ── SaaS を選ぶ場合の最重要項目は，「使いやすさ」──」（プレスリリース）（http://www.csaj.jp/release/08/20080331.pdf）（2008.11.17 確認）
3. 北原佳郎『SaaS は ASP を超えた』，ファーストプレス，2007.8.1
4. 城田真琴『SaaS で激変するソフトウェア・ビジネス』毎日コミュニケーションズ，2007.10.25
5. 前川徹「SaaS の本質を考える」富士通総研 Economic Review Vol. 12, No. 1 2008 年 1 月号，pp. 4–7

SaaS (Software as a Service) and Information Security

Toru Maegawa

SaaS (Software as a Service), a model of software deployment where an application is hosted as a service provided to customers across the Internet, is becoming popular. SaaS has a number of advantages for users. For example, users of SaaS can reduce the operational costs of information systems. According to existing surveys, SaaS users are afraid of information leakage from SaaS venders and stoppage of the service caused by network failure. On the other hand, some users think that they can achieve high reliability and security if the SaaS vender is trustworthy. People who are already familiar with SaaS are more likely to think so. Therefore, expanding the understanding on SaaS reduces user's anxiety about SaaS information security. And it is much more likely that users who choose SaaS for the purpose of improving information security will increase.

Keywords: SaaS, Software as a Service, Information Security