SaaS 向け SLA ガイドライン

平 成 ２ ０ 年 １ 月 ２ １ 日
経 済 産 業 省

発刊に寄せて

これまで日本の中小企業は、「IT 活用の戦略がない」「IT 導入資金がない」「IT スキルを持った人材がいない」などの要因で IT 化が進まないといわれている。経済産業省では、全体で３７２万社[1]といわれる中小企業の IT 化による生産性向上や競争力強化が喫緊に取り組むべき課題と認識しており、「成長力加速プログラム[2]」に沿って、中小企業の多様な課題に対応した「中小企業ＩＴ経営ロードマップ」の策定や中小企業経営者に対する研修、支援体制の強化など、中小企業に対するＩＴ化の支援に集中的に取り組んでいるところである。特に、高度な業務処理サービスをインターネット上で提供する Software as a Service (SaaS[3])は、これら課題を解決し中小企業にとって使いやすい新たな IT サービスを普及・促進する有力な手段と考えている。

SaaS は米国を中心に急速に普及しつつあり、２０１０年に１兆円の市場規模と予想されている。また、日本においても２００４年には、約４，２８０億円、２０１０年には１兆５，３９０億円の市場規模[4]と予想され、海外のサービス事業者をはじめ、既存のパッケージベンダなど、多くの SaaS 事業者が日本市場でもサービスを開始している。

SaaS とは、インターネットを通して必要なアプリケーション（機能）をユーザが利用できる仕組みであり、利用者は自社でシステムを構築、あるいはアプリケーションソフトを購入・インストールしなくても、インターネットに接続された必要条件を満たす PC があれば、ブラウザ経由で財務会計や顧客管理等の業務アプリケーションを利用することができる。つまり、自社の財務や顧客データ等も含めて情報システムはすべて“ネットの向こう側”にあり、SaaS サービスの提供者が維持管理を行っている。

また、SaaS は最新の Web 技術やプラットフォーム技術を利用した情報システムで、一つのシステムを複数の企業で利用する（シングルシステム・マルチテナント方式の）ため、低コストで高度なサービスが提供可能である。SaaS は利用企業ごとに画面レイアウトや表示項目などを簡単にカスタマイズでき、使い方によっては初期導入費用も安く、月額あるいは年額単位で利用ユーザ数（ID 数）に応じたサービス費用を支払う。このため大手企業と比較して IT 投資力が低い中小企業にとっても、SaaS を利用することで比較的低コストで大手企業と同等の IT 環境を整備することができ、近年、日本においても中小企業やサービス業での活用が急速に広がることが期待されている。

一方、インターネット等を経由するサービスであり、また、自社の財務データや顧客データなどをサービス提供者に預けることとなるため、企業が安心して利用するためには、利用者とサービス提供者間で、サービスレベルに関する取り決めが重要である。本ガイド

---

[1] 出典：平成１８年中小企業実態基本調査（平成１９年７月、中小企業庁）
[2] 平成１９年４月２５日経済財政諮問会議決定
[3] Software as a Service の略。「サース」と発音する。本ガイドラインでは、ASP(Application Service Provider)の進化系と捉えており、その定義については第２章「本ガイドラインにおける SaaS の定義」を参照。
[4] 出典：ASPIC ジャパンの資料（市場規模には、セキュリティ・ホスティング等のデータセンタを含む）

ラインでは、SaaS 型取引に係る紛争を未然に防止するために、実際の SaaS サービスにおけるサービスレベル設定事例を元に、利用者とサービス提供者間が事前に合意すべき事項や望ましいサービスレベルに関する指針を示した。

本ガイドラインは、SaaS サービス提供企業、サービスの利用企業、情報サービス産業の業界団体、および学識経験者等に出席いただいた経済産業省情報処理振興課主催の「中小企業のＩＴ化推進のための意見交換会（SaaS・ASP の活用を目指して）」、並びに情報セキュリティに関しては独立行政法人情報処理推進機構（IPA）に設置した「SaaS 利用者の観点からのセキュリティ要件検討会」により検討してきたものである。

本ガイドラインが、SaaS サービスを利用する中小企業およびサポートする IT ベンダや IT コーディネータ、あるいはサービス提供企業ばかりでなく、SaaS に関心のある人々が積極的に活用されることを切に願っている。

経　済　産　業　省
商 務 情 報 政 策 局
情 報 処 理 振 興 課 長
八 尋　俊 英

中小企業のＩＴ化推進のための意見交換会（SaaS・ASP の活用を目指して）　名簿

青野　慶久	株式会社サイボウズ　ＣＥＯ
石田　一雄	富士通株式会社　経営執行役常務
宇陀　栄次	株式会社セールスフォース・ドットコム　代表取締役社長
海野　忍	株式会社ＮＴＴデータ　常務執行役員　ﾋﾞｼﾞﾈｽｿﾘｭｰｼｮﾝ事業本部長
大塚　裕司	株式会社大塚商会　代表取締役社長
小川　健夫	社団法人情報サービス産業協会　副会長 （日立ソフトウェアエンジニアリング株式会社　相談役）
加藤　和彦	筑波大学大学院システム情報工学研究科教授
河合　輝欣	日本ソフトウエア産業協会　会長（ＡＳＰＩＣジャパン　会長）
北原　佳郎	ラクラス株式会社　代表取締役社長
木下　仁	株式会社アールワークス　代表取締役社長
篠原　徹	日本商工会議所　常務理事
田島　瑞也	スタック電子株式会社　代表取締役
東 貴彦	ネットスイート株式会社　代表取締役社長
日高　信彦	ガートナージャパン株式会社　代表取締役社長
眞柄　泰利	マイクロソフト株式会社　執行役専務
松島　克守	東京大学大学院工学系研究科技術経営戦略学専攻教授
丸山　好一	社団法人電子情報技術産業協会　情報・産業社会システム部会委員 （日本電気株式会社執行役員常務）
和田 成史	社団法人コンピュータソフトウェア協会　会長 （株式会社オービックビジネスコンサルタント　代表取締役社長）

目次

1. ガイドライン策定の背景と目的

パーソナルコンピュータの普及とともに、１９９０年代には各企業等においてクライアント・サーバ型の業務アプリケーション（以下、「クライアント・サーバ型」という）が開発、導入され、企業等の IT 化が急速に進んでいった。クライアント・サーバ型は専用のクライアントプログラムが必要であったが、１９９０年代後半から OS にウェブブラウザが標準装備されたことから、ウェブブラウザをクライアントプラットフォームとして利用するウェブアプリケーションが広く導入されるようになってきた。

ウェブアプリケーションが広く普及した背景には、ハードウェア性能の向上、インターネット回線の広帯域化、あるいはシステム開発期間の短縮および運用保守コストの低減による総費用削減など、様々な要因が考えられる。例えば、クライアント・サーバ型では、プログラム開発および変更等において、クライアントとサーバ、双方のプログラムの開発や変更が必要である。しかし、ウェブアプリケーションではサーバプログラムの変更のみでよいため[5]、多数の利用者を有する大規模組織ではクライアントアプリケーションの再インストール等の作業が不要となることで、運用費用を含めた総費用削減およびアプリケーション仕様の迅速な変更が可能となった。

この様な利点を生かし、近年のインターネット回線の広帯域化とともに提供されたサービス形態が、ASP[6]によるオンラインアプリケーションの提供である。企業等が自らウェブアプリケーションを開発するのではなく、ASP が提供するオンラインアプリケーションを、利用者が部分的な設定変更もしくは限定的なカスタマイズを通じて、比較的簡便に利用可能となることが ASP の特徴の一つである。利用者は月額もしくは年額費用を従量制[7]で支払いサービスを利用する。

更に、最近では企業等の業務プロセスに応じて柔軟なカスタマイズや他のアプリケーションとの連携ができるサービスとして SaaS が登場してきた。SaaS とは全く新しいサービス形態ではなく ASP の進化形と考えることができる。

ASP が提供するオンラインアプリケーションを利用することで、利用者は情報システムの初期構築・導入費用を低減でき、またサービス事業者がサービス利用料金内で保守運用を行うことから社内に IT 専門家がいなくても、利用者は容易に情報システムを利用することができるメリットがあった。しかし、ASP が登場した頃はウェブアプリケーションの構築技術が成熟しておらず、使いづらいユーザインタフェースや頻繁に発生する画面の再読込といった機能面での不足があり、またサーバのハードウェア能力の不足からアプリケーションの動作が遅かったり、サービスにおける利用者の不満が ASP の持つメリットを上回り、結果として普及が進まなかったと考えられる。

しかし、ここ数年の急速なウェブアプリケーションの構築技術の発展、完成度の高い開

[5] 特別なプラグインクライアントプログラムを必要とする場合もある
[6] アプリケーションサービスプロバイダ、Application Service Provider
[7] 主には人数×利用期間

発フレームワークの登場、ユーザインタフェースの向上、ネットワークの広帯域化・低廉化、計算機能力の向上、プロセッサのマルチコア化、ハードディスクの大容量化、更には、ビジネスロジックにまで及ぶカスタマイズ機能の提供等、以前に比べて周辺環境が整ったことで、従来の ASP のマイナスイメージを払拭する機能および性能を提供できる ASP を提供することが可能となった。これが、すなわち SaaS の誕生といえる。

SaaS が提供するオンラインアプリケーションは、インターネット経由でアプリケーションを利用するためインターネット回線の品質やトラフィックが集中した際の性能低下、不正アクセスによる情報漏えいなど情報セキュリティ上の懸念、利用者の要求に応じたカスタマイズ部分から問題が発生した場合の責任分解点、あるいは業務データを第三者の SaaS 事業者に任せるというサービス利用上の懸念といった課題が存在する。

そのため、SaaS が提供するオンラインサービスを利用する際には、サービス提供企業と利用企業間での、サービス内容・範囲・品質等に関する保証基準の共通認識であるサービスレベル合意（Service Level Agreement : SLA）を得ることが、当事者間の適切な取引関係を確保し、SaaS の普及を図るため、非常に重要である。

本ガイドラインでは、企業の経営者および情報システム担当者が SaaS を利用するにあたって適切な取引関係を確保し、より効果的に利用することを目的に、情報セキュリティ確保の観点に重点を置き SaaS の特徴について解説し、利用するサービスおよびサービス事業者選定の際に参考となるような利用者への対策向上のガイドラインを提供する。

なお、本ガイドラインの対象は企業等の利用者であり、契約に基づいてセキュリティを初めとするサービスレベルを確保することを想定している。

1.1. 本ガイドラインの利用について

本ガイドラインでは、SaaS という新しい用語の定義を示した上で（第二章）、その実際の適用事例を示し（第三章）、SLA の重要性（第四章）、SLA の内容（第五章）、SLA の確認事項（第六章）を示す。更に、利用者が SaaS 導入に向けて準備しておくべきことを記述している（第七章）。

本ガイドラインの利用に際しては、まず、第一章、第二章で示している SaaS の特徴等について十分に理解し、その上で、第三章にてサービス毎の適用状況を把握し、第四～六章で述べる SLA の内容等を考慮しつつ、SaaS 提供者選択に利用することを想定している。

なお、本ガイドラインは、日本における SaaS ビジネスの市場拡大、技術進展等の状況を踏まえて、必要に応じて適宜改訂を行うこととする。

2. 本ガイドラインにおける SaaS の定義

SaaS は比較的新しい用語、概念であり、用語の定義が明確でないことから、まず本ガイドラインにおける SaaS の定義を示す。また、定義を示すことで利用者環境における SaaS 導入メリットおよびデメリットについてもおのずと明確になるものと考える。

2.1. SaaS と自社所有システム

本ガイドラインにおける SaaS とは「インターネット経由でアプリケーション機能を提供するサービスの形態」を指す。最も一般的な SaaS の形態は、SaaS 提供者が提供するウェブアプリケーションを利用者がウェブブラウザを通じて利用する形態[8]である。

SaaS 提供者が提供するサービスには、アプリケーション機能に加え、システムの管理および運用、利用者に対するヘルプデスク業務なども含まれている。

従来は、アプリケーションを利用するために利用者の組織がシステムインテグレータ（以下、SIer[9]）等に対価として開発費を支払い、完成したシステム一式を受け取るという所有して利用する形態をとっていた。SaaS を利用する場合においては、企業は利用者数や規模に応じたサービス利用料金を支払い、必要なだけサービスを利用することができる。このように所有せず利用することで、一般的には支出を抑えることが可能だといわれている。

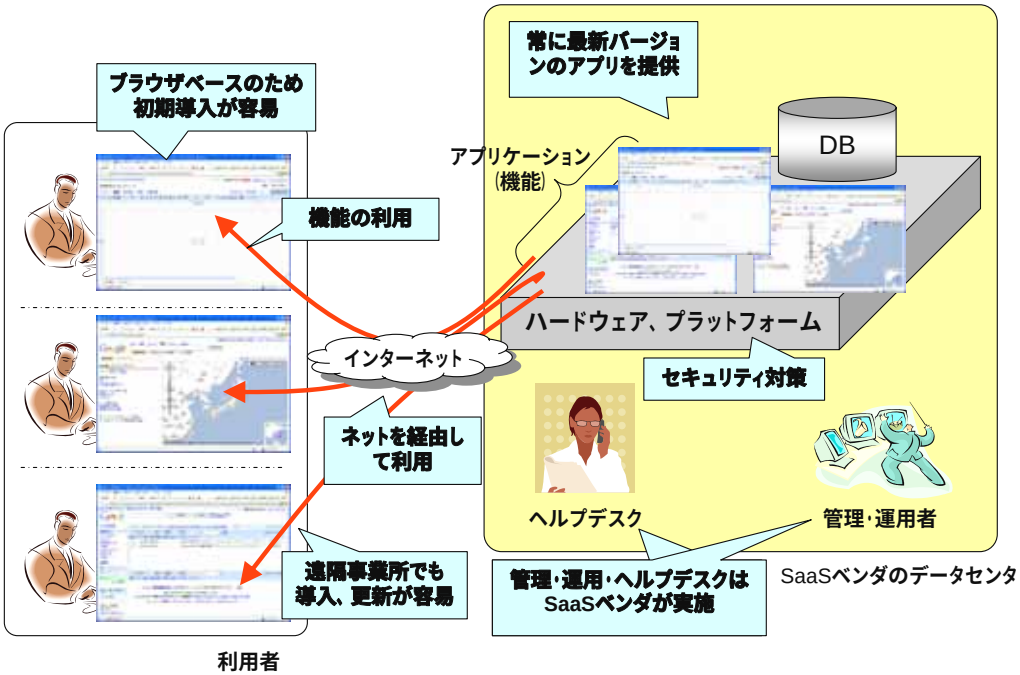

図 1　一般的な SaaS のイメージ（システムを利用する場合）

[8] SaaS を広義に捉えると、月額で利用料金を払い、利用者のパソコンにクライアントプログラムをインストールし、データセンタのサーバ上にあるデータを利用したりクライアントプログラムを更新する形態もあるが、本ガイドラインではウェブブラウザを通じてアプリケーションを利用する形態の SaaS を中心に解説する。

[9] System Integrator

一方、SaaS 以外のシステムとは自社でシステムを所有する形態を指す。すなわち、自社あるいは SIer に業務委託を行い、システムの要件定義や設計を行って開発するか、パッケージ製品を自社の業務や仕様に合わせてカスタマイズを行い、システムを構築するなど、企業が自社でシステムを所有する形態である。仮にウェブインタフェースのシステムでも SIer から納品され自社でシステムを所有する場合は、SaaS には含まれないものとする。

システムを所有する場合、自社の業務に合わせて最適なシステムを構築可能であるが、クライアント PC 以外にもサーバやアプリケーションソフト等を自社で用意する必要がある。また、自社で管理・運用する場合には、利用者からの問い合わせ対応をするヘルプデスク、設備、サーバ等システムの管理や運用などの作業、管理・運用要員の確保など実施体制の整備も必要である。しかし、SaaS の場合、カスタマイズの範囲は制限を受けるが、導入が容易であり、社内に IT 専門家がいなくても利用できるなどの特徴がある。

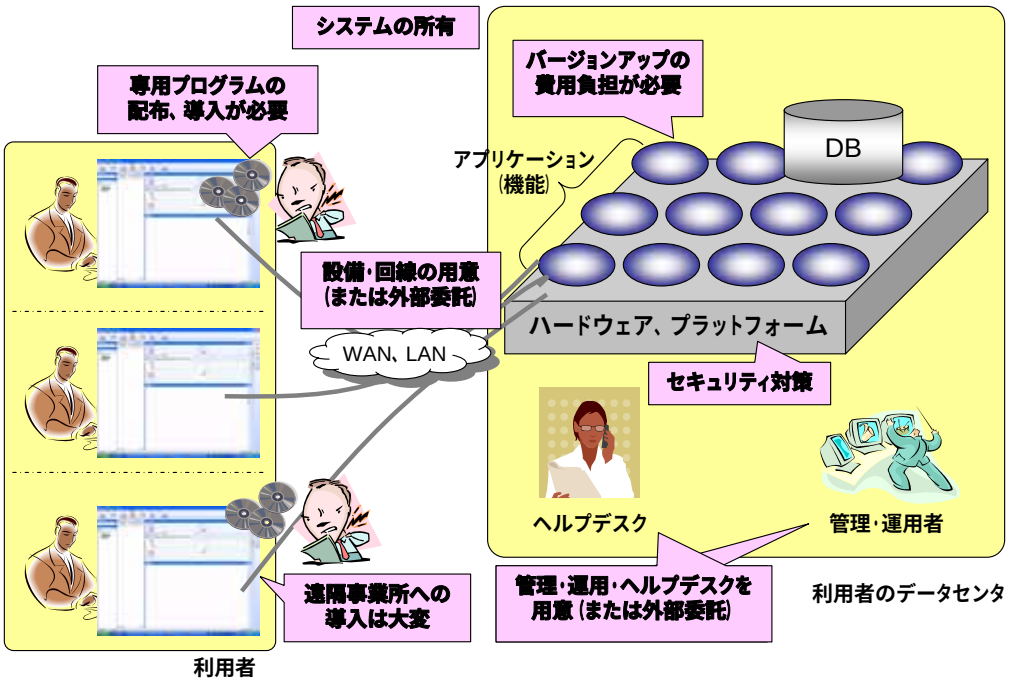

図 2　自社所有システム、パッケージソフトのイメージ（システムを所有する場合）

いずれの形態であれ、システムを導入し効果的に活用するためには、事前の業務分析、システム適用範囲や手法の検討および決定などの事前検討プロセスは必要な作業である。

具体的には、以下の検討が必要となる。

- 業務プロセスの現状分析と改善策の決定
- IT 責任者の選任と教育（SaaS の場合でもクライアント PC の管理要員は必要）
- 情報モラル教育の徹底
- 危機管理体制の明確化（障害時の業務の継続方法、情報漏えい時の対応など）

すなわち、これら事前検討を踏まえて、SaaS 形式と自社所有形式の特徴を理解した上で、どのような形態でシステムを導入するかを決定する必要がある。

ここでは、パッケージソフトを自社所有形式の具体例とし、一般的な SaaS 形式との特徴比較を表１にまとめる。

	SaaS 形式	自社所有形式 （パッケージソフト）
システムの所有／利用	利用	所有
システム設備の自社負担	常時接続のインターネットとクライアント PC	左記に加えて、サーバ、アプリケーションソフト、データセンタ設備など
事前検討	業務分析、業務設計／見直し等が必要。（外部に委託する場合は、コンサルティング費用が必要）	同左
アプリケーション開発 （基本機能）	SaaS 提供者が提供する基本システム／機能	パッケージベンダが提供する基本システム／機能
アプリケーションの カスタマイズ	顧客の要望により、範囲の制限があるがカスタマイズが可能（要求仕様を示して画面やデータ項目表示名等を作成することなどが必要）	顧客が自社に合った仕様を提示し、プログラムのカスタマイズが可能（基本的には、SIer 等によるカスタマイズ開発を伴う）
初期導入（システム）	・ネットワーク環境およびクライアントの準備 ・ネットワークおよびクライアントのセキュリティ対策の実施 ・また、他のアプリケーションと連携する場合は、連携部分の作り込みが必要	・サーバおよびクライアントの双方の導入が必要 ・ネットワーク、サーバ、およびクライアントのセキュリティ対策の実施
初期導入（その他）	利用者の操作および情報モラル教育	・システム開発の専任要員の確保・育成 ・利用者の操作および情報モラル教育
クライアントの管理	セキュリティの観点から OS など PC ソフトを最新の状態に保持する	左記に加えて、アプリケーションソフトのバージョンアップ作業などが必要
メンテナンスのタイミング（サーバ側）	SaaS 提供者に依存	利用者の都合でメンテナンス期間や時間を設定
管理者、ヘルプデスク	基本操作に関する管理者やヘルプ対応要員は必要	システム全般の管理やヘルプ要員が必要
セキュリティ	・クライアントの管理は必要 ・アプリケーションは SaaS 提供者がセキュリティを確保	すべて自社での対応
運用管理	・クライアントの管理は必要 ・アプリケーションは SaaS 提供者が運用	すべて自社での対応 （第三者ベンダに外部委託する場合もあり）
費用	サービスの提供内容に即したコストの負担	将来の拡張性等も考慮した、余裕を持った設備投資が必要

表 1　SaaS 形式と自社所有形式（パッケージソフト）の比較

2.2. SaaS の歴史

SaaS はインターネット経由での利用を前提としている。インターネットの誕生は米国における１９６０年代後半の ARPANET[10]の誕生にまでさかのぼるが、本章ではウェブブラウザが一般的に使用されるようになった１９９８年頃から現在に至るまでの歴史をウェブブラウザの普及、接続環境の向上、操作性の向上の観点から解説する。

- **ウェブブラウザの普及**

SaaS アプリケーションは基本的にウェブブラウザをプラットフォームとして利用するものである。国内においては、一般的に利用されるクライアント OS として１９９８年にマイクロソフト社から Windows 98 が発売され、Netscape Navigator や Internet Explorer などウェブブラウザが標準的に使える環境が整った。これ以降、利用者はメールソフトやメモ帳と同じ感覚でウェブブラウザを利用できるようになった。

現在では、携帯電話等にもウェブブラウザが標準装備されており、SaaS のクライアント環境はパソコンのみならず携帯電話、PDA にも広がっている。

- **インターネット接続環境の向上**

ウェブブラウザとともにインターネット接続環境も SaaS を利用するための必須条件である。インターネットが一般的に利用されるようになってきた１９９８年頃には、比較的低速なアナログ回線や ISDN 経由で必要に応じて ISP に接続・切断していたが、その後、ADSL や VDSL などの xDSL と呼ばれる公衆電話回線を利用した高速接続環境が提供されるようになり、加えて回線使用料金も従量制から月額固定の定額制が広まったことでインターネット常時接続環境が実現した。

xDSL が普及する以前でも専用線接続や高速イーサネットによる高速常時接続環境は提供されていたが、現在と比べると遙かに高額であったため一部のネットワーク専業企業や多事業所展開をしている大企業の利用が大半であった。更に、現在では光ケーブルを利用した更なる高速接続環境が安価で利用できるようになり、無線 LAN のフリースポットや PHS や携帯電話などを利用して、外出先や移動環境からでも高速で低廉なインターネット接続が可能となっている。

- **技術進化による操作性の向上**

クライアントの操作性を向上させる技術の進化も SaaS への発展を後押しした。当初のウェブアプリケーションはデスクトップアプリケーションと比較して表現力に乏しい HTML[11]のみで表現されたものであり、入力インタフェースもマウスを有効に活用したもの

[10] 1969 年、米国国防総省高等研究計画局にて研究が行われたコンピュータネットワーク。
[11] HyperText Markup Language（ハイパーテキスト・マークアップ・ランゲージ）：ウェブ上のドキュメントを記述するためのマークアップ言語

ではなく、キーボードタイピングが中心でのユーザインタフェースのみであった。しかし、現在では、様々な技術の発展[12]により表現力や利便性を大きく向上させている。

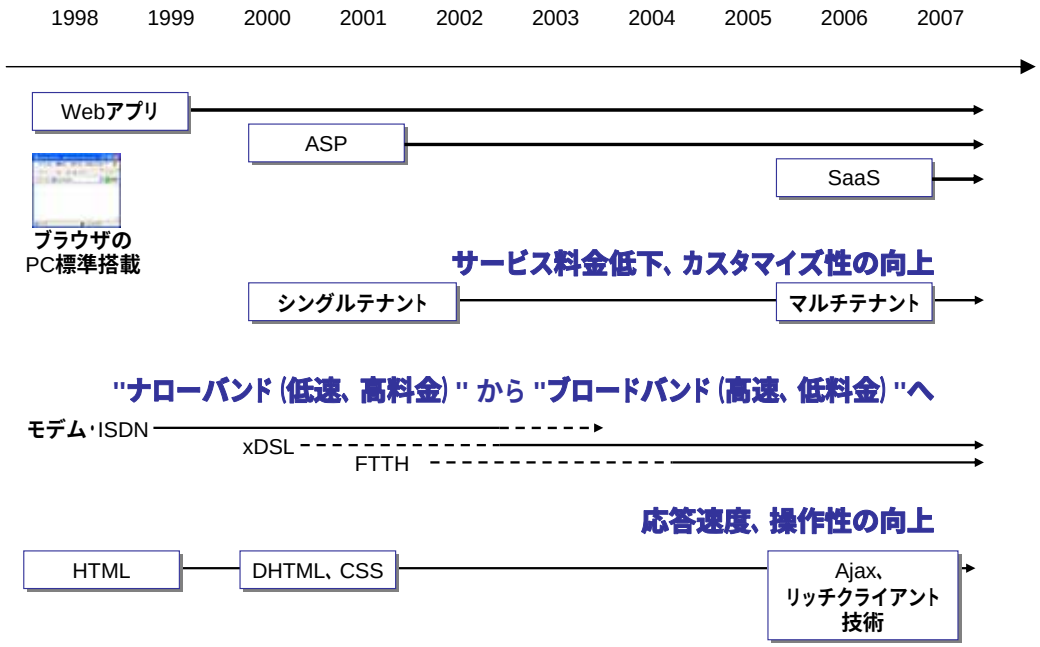

図 3　SaaS に至るまでの歴史

2.3.　SaaS の特徴

要件定義、仕様策定、設計、開発、あるいはパッケージ製品導入等のプロセスを経てシステムを所有する場合と、SaaS 提供者からシステムをサービスとして利用する場合の導入、運用面における費用、期間、機能などを比較し、SaaS の特徴について記述する。

- **初期導入期間における比較**

SaaS を利用する場合は初期データの登録、利用者の教育などを考慮しても２～３ヶ月程度で利用開始できる場合が多い。初期導入期間が短いことにより、新規事業の立ち上げやビジネス環境の変化への俊敏な対応が可能となることから、より多くのリソースを本来業務に投入することができる。

また、サービスによっては機能制限の少ない試用期間が設けてあり、無料で小規模な試用を行い自社の要求に適合していると認められた場合には、そのまま本採用という形態を採ることができるため、試験導入期間のデータを有効に活用することができる。

一方、新規にシステムを開発する場合には業務分析、要件定義、設計、開発、試験、導

[12] Dynamic HTML、CSS（Cascading Style Sheets：カスケーディング・スタイル・シート）による表現力の向上、Java Script の有効活用によるインタラクティブ性の改善、更に Ajax や Adobe Flash などのリッチクライアント技術の進化によるマウス中心の入力インタフェースの実現や度重なるページの読み込みの回避等により利便性を大きく向上

入、運用という工程を経るため、規模にもよるが導入までに長い期間かかる場合もある。また、パッケージ導入の場合でも、パッケージの機能と自社のビジネスルール、業務フローなどの違いを確認する調整作業、プログラム改修を伴うカスタマイズなどの工程などは半年以上かかる場合もある。

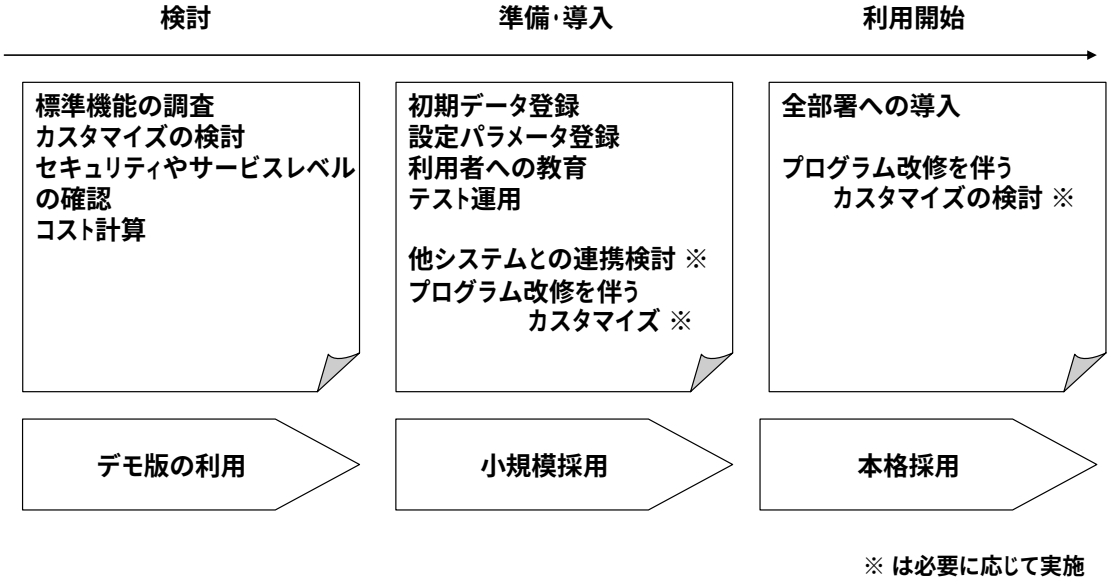

図 4　SaaS 導入フロー

- **費用面における比較**

システム開発を SIer に委託した場合やパッケージ製品の導入などシステムを所有する場合に比べれば、SaaS の初期導入費用は一般的には安価になると考えられる。ランニングコストについても利用者数に応じたサービス利用料金であるため、利用者数が少ない場合はハードウェアやデータセンタ設備等の管理や運用業務にかかるコストを考慮すれば安価になるが、利用者数が増えると全体のコストでは高価になるのが一般的である。また、ハードウェア、アプリケーションなどのアップグレード、セキュリティ対策費用なども当初に契約しておけば追加負担も不要である。ただし、カスタマイズ費用に関しては一概にシステムを所有する場合との比較は困難である。また、多数の利用者で長期間にわたって利用する場合は、割高になるケースもある。

しかし、経営という観点から見た場合には、新規システム構築やパッケージ導入などのシステムの所有は対象業務の規模が拡大するという前提で構築するため、回線設備、インフラ面はどうしても先行投資になりやすい。SaaS では、システムの利用は企業規模と利用期間に応じたコスト負担が継続的に発生するが、経営者にとっては企業成長や戦略に合わせたシステムコスト計画が立てやすいというメリットがある。

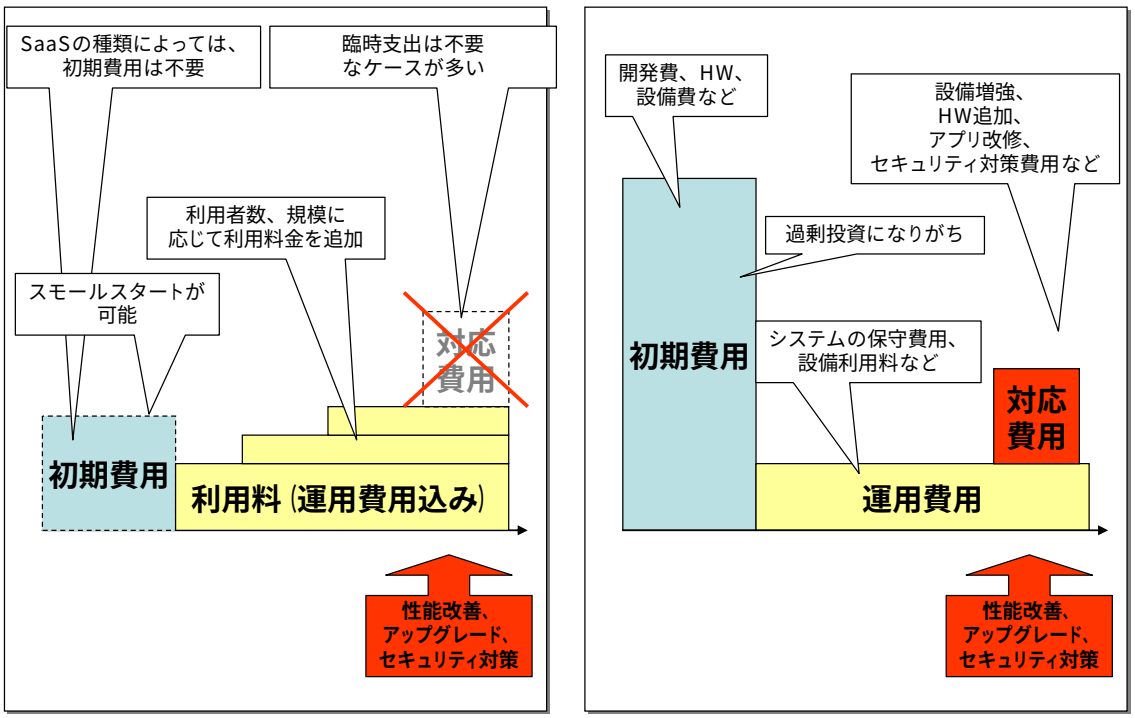

図 5　SaaS と従来システムの費用イメージ

- **運用体制における比較**

SaaS はシステム（設置設備、ハードウェア、アプリケーション等）の機能追加、性能向上、安定性向上のためのアップグレードに関わる業務、領域管理、性能管理、稼働管理等の全体的な管理、運用業務等、すべてがサービスの利用料金に含まれていることが多いため、利用企業はシステムの稼働管理、障害時の復旧、セキュリティパッチの適用などの業務から解放される。したがって、利用企業は追加開発、システム管理、運用のための体制（業務を遂行するためのシステム、担当者のアサイン、教育など）等を契約によっては、負担する必要がなくなる。このことは、費用面でも述べたが追加負担を伴わずに計画的なシステム利用を可能にすると考えられる。

また、SaaS 提供者によっては、利用者への教育、ヘルプデスクなどの設置などもサービスに含まれている場合もあるため、更に利用企業等の業務面での負担は軽減される（費用は別途発生することが多い）。

- **SaaS 提供者に依存するセキュリティ対策と継続性**

SaaS を利用するということは、自社のデータを外部に預けるということであり、SaaS 提供者のセキュリティレベルがデータの安全性を大きく左右する。しかし、セキュリティ対策を十分に実施していない自社サーバでの運営の方が、外部からの不正アクセス、社員による故意あるいは過失による情報漏えい等のリスクは高いと考えられる。そのような場

合、セキュリティレベルの高い SaaS を利用する価値は大きい。また、サービス利用の継続性が、SaaS 提供者の存続性に連動するため、提供者を慎重に選ぶ必要がある。

具体的な選定基準や重要性は後述するが、SaaS 提供者の提示するサービスの品質や保証条件などを盛り込んだ合意書である SLA（Service Level Agreement）や企業の財務諸表、可能であればセキュリティポリシの内容、データセンタの堅牢性、インターネット接続回線、ハードウェア、ソフトウェア等のインフラ、アプリケーションのセキュリティ対策状況等を加味しながら慎重に問題がないことを確認し契約すること。

また、重要な業務や機密度の高い情報を扱う場合と、そうではない場合とでは、SaaS 提供者を選定する条件を分けて検討すること。

- **データ保護に係る特徴**

重要な業務や機密度の高い情報を扱う場合、暗号化通信が必須となるが、SaaS を利用する場合、データが常に SaaS 提供者のサーバにあり、加えて他のサービス利用企業の情報と同じデータベースに蓄積されることもあるため、データの格納形態や SaaS 提供者従業員によるデータのアクセス可能範囲、アクセス時の承認プロセスなどに関するセキュリティ対策を確認することが重要である。

利用者として考慮すべきことは、データの格納形態（分散化、暗号化有無など）の確認、障害時の復旧範囲（復旧できるデータとできないデータの種類）、復旧に要する時間、自社のデータにアクセス可能な提供者スタッフ数の最小化、アクセスできるデータの範囲などに関して SaaS 提供者と取り決めを事前に締結しておくことが大切である。

- **アカウント管理に係る特徴**

SaaS はインターネットで提供されているサービスであるため、誰でもインターネット上からサービス利用の窓口となるログインページへアクセスすることができる[13]。ドアのピッキングツールのようなログイン画面からパスワードを不正に搾取するためのツールが存在するため攻撃者がなりすまし目的で不正ログインを試みるリスクが存在する。このような脅威に対して、連続したログイン失敗時の処理方法（該当アカウントでは一定時間ログインできなくなるようにする、加えて証跡（ログ）の保存、管理者への通知、回復手順等）や、パスワードの桁数、使用可能文字種、有効期限、履歴管理など自社で規定したパスワードポリシ（ルール）が適用可能であるか否かを確認しておくこと。

- **システム間連携に係る特徴**

現在提供されている SaaS アプリケーションの中には外部インタフェース API[14]

[13] ログイン画面にアクセス制限をかける、VPN（Virtual Private Network）経由でしかアクセスできないようにする等の対策がとられる場合もある

[14] アプリケーションを外部から呼び出す、利用するための手続きであり、実態は関数の集合体のプログラムである

（Application Programming Interface）を提供し、この API を利用して異なるシステムやアプリケーション間の有機的な連携が可能なものもある。しかし、システム間連携を実現するには、連携部分の作り込みが発生するため、自社でシステム開発要員を確保して開発するか、SIer 等に開発を委託する必要がある。

また、現在提供されている SaaS アプリケーションの API は、各ベンダが独自に定義していることから、既存システムや他社 SaaS アプリケーションとの連携が必ずしも可能とは限らない。既存システムから SaaS アプリケーション内のデータ参照は、SaaS アプリケーションが提供する API の範囲内では可能であるが、SaaS アプリケーションから既存システムへの参照は既存システム側に内部データの操作を想定した API が整備されていない限り困難である。

つまり、販売管理は A 社の SaaS、生産管理は B 社の SaaS を利用している場合でも、共通の API やデータ構造を持たない限り A 社の販売管理 SaaS から B 社の生産管理 SaaS で管理している工場在庫データを直接検索するようなシステム間連携は困難である。

特に、自社にシステム開発要員を持たない中小企業の場合には、システム間連携については、実現可能性、費用対効果、あるいはシステム開発の委託先などを鑑みて、判断する必要がある。

- **カスタマイズに係る合意事項**

SaaS は、パラメータ化などの手法を用いることにより、基本的にはプログラムの改修を伴わず設定変更レベルの作業でカスタマイズが可能である。既存システムや ASP で提供されるアプリケーションのカスタマイズに比べて、より簡単にカスタマイズが可能である場合が多い。

しかし、設定変更レベルのみで要望する全ての機能を実現できるわけではない。したがって、将来的な利用用途や業務拡大などで追加で必要となる機能がわかっている場合には、提供されるカスタマイズ機能で実現可能かどうかを事前に検討しておくことも必要となる。また、個別のカスタマイズが発生する場合には、その必要性、実現性あるいは対応コスト等について SaaS 提供者と協議して合意しておく必要がある。

また、自社の業務に合わせて SaaS をカスタマイズするのではなく、一つの選択肢として、SaaS で提供される標準的な業務フローを取り入れることを検討することも重要である。

- **サービス終了時のデータ移行に係る確認事項**

SaaS の利用を終了する際に、SaaS 提供者に蓄積されているデータから新システム又は次の SaaS への移行を行う必要がある。SaaS の導入検討時に次のシステムへの移行を具体的に想定することは困難であるため、移行する際に必要になると予想されるデータの権利面（利用期間中に入力したデータや入力データから集計、加工されたデータなどを契約解消時に受け取る権利、SaaS 提供者は契約解消後の確実な消去、あるいは合意した範囲以外

に利用しないなどのデータの取り扱いを定めた権利)、機能面での出力可否、CSV（Comma Separated Values、カンマ区切り形式）などの一般的なフォーマットによるデータ出力の可否の対応状況などを事前に確認しておくことが望ましい。

- **オフライン時の利用に係る事前検討**

一部の SaaS はオフラインでの利用に対応しているが、ほとんどの SaaS はインターネットに接続している状態でしかアプリケーションを利用することはできない。また、オフライン時に対応している SaaS においても機能制限がある場合が多いため、想定する利用形態について事前によく検討する必要がある。

2.4. SaaS に対する利用者の期待

SaaS は当初から順調に普及していったのではなく、旧来の ASP と呼ばれている間は、一部のサービスを除いては思うように利用が拡大していかなかった。しかし、以下で説明する利用者のニーズを満たしていくことで発展を遂げてきたと考えられる。

- **コストダウン**

SaaS 提供者は一つのシステムで複数利用者組織の情報やアプリケーションを管理するマルチテナントと呼ばれる技術を応用している。このマルチテナント技術の応用により、SaaS 提供者はシステムの利用効率を最大限にすることができ、管理および運用コストを最小限に抑えることが可能となった。その結果として SaaS の利用料金を下げることに成功したといえる。ただし、マルチテナントは、１つのシステムを複数の利用者で共有するため、サービス提供時間など利用者個別の SLA を設定できない項目もある点に留意すること。

マルチテナントが可能になった背景としては、ブロードバンドの普及による利用者 PC と SaaS アプリ間の通信量およびアクセス頻度の増加に対応が可能なインフラの進化、サーバの仮想化技術、企業の違いに対応するためのアプリケーションの動作、画面表示等をパラメータにて変更可能とし、その変更のみでプログラム改修を伴わずに企業個別のカスタマイズを可能にするアプリケーション開発技術の進展等が挙げられる。

一方、従来の ASP と呼ばれる方式は、アプリケーションのサービス提供形態をインターネット経由にすることで従来のパッケージ導入や自社開発と一線を画したが、データ管理はシングルテナントと呼ばれる利用企業ごとにシステム一式を個別に用意する方式であった。そのため、ハードウェア購入費用や管理および運用コストを追加負担する必要があり、結果的に安価なアプリケーション利用料金を実現することが困難であった。

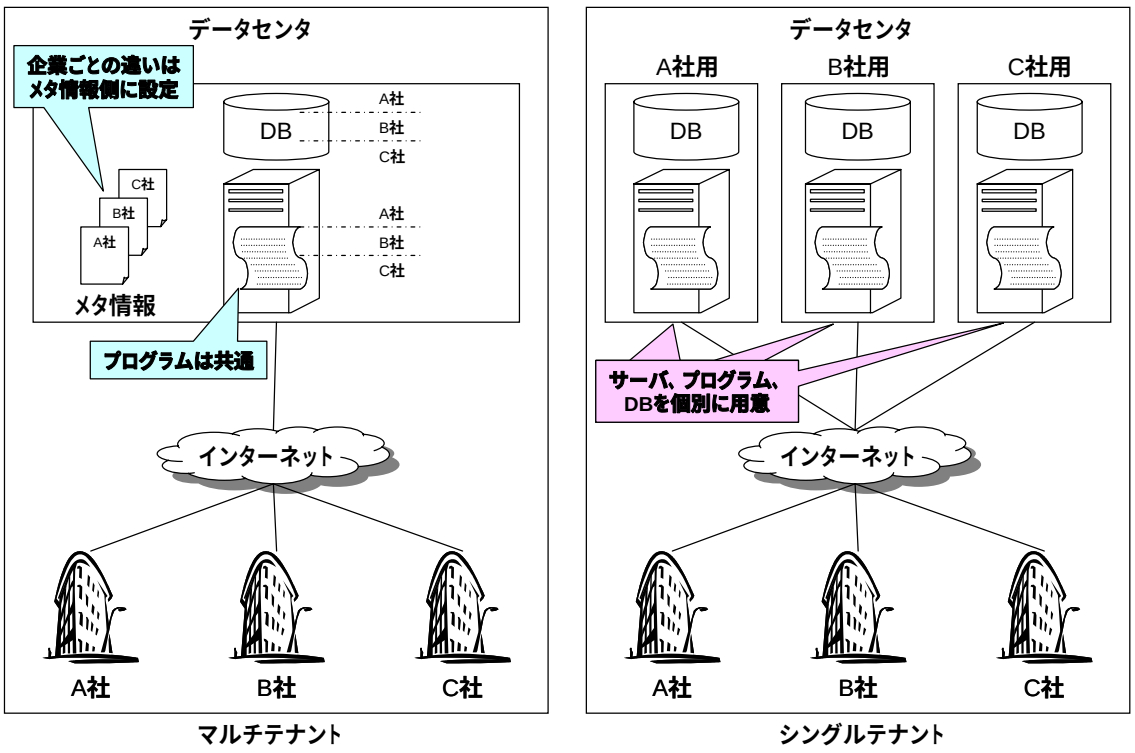

図 6　マルチテナントとシングルテナントの違い

- **ビジネススタイルへの柔軟な対応**

予め備えている標準機能では自社のビジネスプロセスやルールに合わず、アプリケーションをカスタマイズせざるをえない事例は SaaS においても想定できることである。

SaaS アプリケーションによっては、アプリケーションの表示色、フォント、言語、計算ルール、データ構造、処理フローなどの情報を変更可能なパラメータとして管理することにより、利用者が自立的に設定できるものもある。この機能により、カスタマイズ範囲の制限はあるものも、企業毎に異なる業務プロセス、帳票に表示すべき項目、並び順などのビジネスルールや扱う情報の名前や型、種類の違い、入出力画面などユーザインタフェースなどを、利用者に合わせてカスタマイズすることも可能である。

例えば、管理するデータを追加し項目名を自由に定義できることで、従来の ASP やパッケージであればデータベースのスキーマ変更やサーバ側のプログラムの改修が必要だったカスタマイズ作業が、パラメータ設定により容易に変更可能になっているものもある（一部の優良なパッケージ、ASP でも同様にプログラムの改修なしにカスタマイズが可能ではあるが、一般的にはプログラムの改修が必要なものが多い）。

このように短時間で要望に沿ったシステムを開発し、とりわけ入出力画面設計などユーザインタフェースのカスタマイズが短時間に低コストで実現できることは、利用者にとって大きなメリットである。

- **優れた操作性**

SaaS アプリケーションは、ウェブブラウザベースで動作するものがほとんどだが、Ajax やリッチクライアントなどの最新技術を採用することで、直感的に操作可能なユーザインタフェースを提供し、クライアントアプリケーションと同様の利便性を実現している。

図 7　直感的なユーザインタフェース

以上のように、利用者のニーズに対応することで SaaS は発展してきた。言い換えれば、旧来の ASP はインターネット接続環境のようなインフラ環境的な要因もあるが、利用者のニーズを満たせなかったため普及することができず、ニーズへの対応を可能とする現在の SaaS へ進化を続けているのである。

3. 適用分野別の SaaS 利用事例

ブロードバンドの普及に伴いインターネットは社会インフラとして定着し、インターネットを有効活用して、今後ますますアプリケーションの SaaS 化は加速すると思われる。SaaS はシステムを所有する場合に比べて準備・検討に要する期間・費用が一般的には安価に抑えられ、かつ企業規模に応じたコスト負担となるため、特に中小企業にとっては非常に魅力的であろう。

しかし、すべての業務システムを SaaS アプリケーションに置き換えることは、企業の競争力を減退させる可能性もあるため慎重な検討が必要である。一般的に SaaS の導入を慎重に検討すべきアプリケーションは、企業の競争力の源泉となっているシステムに関わる分野である。競争力の源泉となる部分は企業独自のものである場合が多いため、プログラムの改修を伴う大幅なカスタマイズが必要になるケースが多い。例えば、製造業における生産管理、原価管理、小売業における販売管理、売上予測、SCM（Supply Chain Management）などに関わるアプリケーションである。ただし、利用を検討している SaaS が予算内の導入コスト以下で自社の独自性を含む要件を実現できる場合、SaaS を導入しても何ら問題はない。

ただし、上記のような基幹業務のシステムが未導入の場合、SaaS 活用による生産管理の改善や SaaS 形式の EDI[15]の活用による受発注業務の効率化など、SaaS 導入による中小企業のメリットは大きい。

一方、SaaS の利用が適している分野は、企業の独自性が含まれているとしても、本質的な部分は他社と変わらない分野である。例を挙げると、グループウェア、CRM（Customer Relationship Management）、ワークフロー（人事・給与、記帳・会計等）等である。従来からこれらの分野はパッケージの導入が進んでいたが、今後は SaaS への移行がより一層加速されることが推測される。

以降は、主な SaaS のサービス分野を説明する。

3.1. ビジネス系サービス

- CRM、SFA（Sales Force Automation、営業支援）サービス

CRM や SFA は、商材、取引先、商談情報などの管理や売上予測などの機能を持ち、効率的な営業活動を支援するツールである。外出が多い営業担当者にとっては、インターネットに接続さえできれば、場所を選ばずリアルタイムに営業情報の登録、閲覧が可能になることは大きなメリットとなる。

主な事例としては、大手メガバンクグループのシンクタンクや日本郵政グループが CRM

[15] Electronic Data Interchange（電子データ交換）：企業や行政機関などがコンピュータをネットワークで繋ぎ、伝票や文書など商取引に関する情報を標準的なフォーマットの電子データで、自動的に交換すること

アプリケーションの導入を決定したケースがある。

- **人事情報管理・給与計算サービス**

人事情報管理および給与計算は、あらゆる企業に共通して存在する業務ではあるが、企業ごとに異なる人事規程や文化に即した細かい要件に対応する必要があり、SaaS の適用に際してはカスタマイズ性をよく検討することが望ましい。

また、単なる機能提供にとどまらず、業務のアウトソーシングに至るまでサービスとして提供している提供者もあり、企業はシステムを用意する必要がなくなる上に人事担当者の事務的な業務負担が軽減され、採用や人材育成などの分野に注力することが可能になる。

主な事例としては、ホワイトカラー中心の企業向けに、人事情報データベースやワークフローなどの機能を導入したケースがある。これらのソフトウェアが SaaS として利用できるだけではなく、給与計算、社会保険手続きや従業員との個別対応、外部機関へのデリバリー等企業の担当者が行っている業務をすべてアウトソーシングすることも可能である。

しかし、例外ケースや給与分類の多い企業への適用については、事前検討を十分に行わなければならない。

- **会計・記帳サービス**

財務会計や税務申告に必要な帳簿の出力などの機能をもった分野もまた、あらゆる企業に共通して必要な業務である。人事情報管理・給与計算サービスの分野と同様に、業務のアウトソーシングまでサービスに含めて提供される場合もある。

以上の分野は、米国における分野別提供者数の上位を占めている分野であり、日本においても、同様のサービスが、現状では主に中堅企業を対象に提供され始め、今後より広い範囲への応用が期待されている。

3.2. IT 系サービス

- **メールサービス**

利用者の追加作業（メールアカウントの登録作業）を行うことにより、即座にメールシステムの利用が可能となることは、従業員数の変動（採用、退職等）に伴う業務の遅れが生じないため運用面で大きなメリットがある。SaaS 提供者からドメイン[16]が提供される場合、あるいは独自ドメインの利用ができるサービスも提供されている。加えて、ウイルスチェック機能やスパムメール対策などのセキュリティ対策機能が付加されているサービスの場合は、ワンストップで必要な機能とセキュリティ対策が提供されるため利用する企業にとってはセキュリティにおける特別な配慮が不要であるとともに、パターンファイルの

[16] 電子メールアドレスの@以降の部分のこと

更新等の運用作業が不要となる等、運用コストにおいてメリットがある。

主な事例としては、日本大学がメールサービスを導入し、学部ごとに異なっていたメールシステムを統合したケースがある。

- **コラボレーションツール系サービス**

Wiki、スケジュール・設備予約管理、ToDo 管理、掲示板、オンライン会議、e ラーニングなど様々なコミュニケーション機能を備えたコラボレーションツールにおいて、移行作業は主に利用者のアカウント登録であり比較的負担が軽く、その上、従業員にとって身近な機能であるため非常に利用しやすい。

- **セキュリティ対策サービス**

インターネットの常時接続が一般的となった現在、企業内のサーバ、クライアントマシンでのウイルス・スパイウェア対策、パーソナルファイアウォールの導入、ウェブフィルタなどのセキュリティ対策は企業内のネットワーク環境を安心・安全に利用する上で不可欠である。

従来は目的別にセキュリティ製品を導入するか又は UTM（Unified Threat Management）製品[17]を導入し、専門の担当技術者を用意することによって管理・運用する必要があり、担当技術者には高度なセキュリティ知識が要求されていたため、人材育成や確保は容易ではないと考えられていた。しかし、SaaS を利用することで、セキュリティに詳しい技術者が組織にいなくとも、一定のセキュリティレベルを達成することが可能となった。

- **PC ヘルプデスクサービス**

一定の規模以上の組織にとっては、オフィスで使用している PC のヘルプデスク対応は組織的な対応が必要になる。この分野では、クライアント側に特別なソフトウェアをインストールせずに、リモートからのチャットや画面操作を提供しているものがあるため、担当者の育成や複数事業所に対する長時間のヘルプデスクサービス提供に課題を抱えている企業にとってはメリットがある。

- **ID 管理・認証などの基盤系サービス**

SaaS 提供者の設備、ネットワーク環境などに障害がなく、安定して SaaS が利用できるという前提に立てば、社内のアカウント管理（ID、認証情報、権限情報などの管理）のインフラとして SaaS を利用する、つまり他の既存システムから SaaS の認証 API を経由す

[17] アンチウイルス、不正侵入検出、ファイアウォール等、複数のセキュリティ機能を統合的に管理する製品のこと

るシングルサインオン[18]環境を構築することは、独自でシングルサインオン環境を用意することに比べてコストを安価に抑えることができるとともに、短期間に環境を構築できる可能性が高くメリットが大きい。

しかし、ネットワーク障害、提供者システム障害発生時に SaaS を利用した認証、シングルサインオンサービスが停止、あるいは利用不可能となり、認証機能が連携する既存システムも同時に利用不可能になるリスクも想定する必要がある。また、万が一、SaaS 提供者に預けた認証情報が外部に流出した場合には、その情報を悪用した第三者によるなりすまし被害のリスクが高くなるため、アカウント情報や認証情報の再登録を早急に実施する体制について、事前に構築、確認しておく必要がある。

3.3. 共通する注意事項

- **大幅なカスタマイズを必要とするケース**

2.3 章「SaaS の特徴」の“ ビジネススタイルへの柔軟な対応 ”でも記述したとおり、SaaS はカスタマイズしやすいことが特徴の一つだが、サーバ側のプログラムのカスタマイズではなく、ウェブブラウザのプラグインを活用した入出力画面のカスタマイズやパラメータでの設定変更に限定される。一般的にプログラムの改変を伴うパッケージ・ソフトウェアのカスタマイズと、SaaS のカスタマイズでは根本的に作業内容が異なる。

しかし、独自の商習慣や業務プロセス、管理方式などを SaaS アプリケーションに反映させる場合は、上記のような SaaS 提供者が想定しているカスタマイズの範囲を超え、結果的に多額のカスタマイズ費用や特別に保守費用やメンテナンス費用が必要となることが想定される。このような場合、レスポンスの低下、保守や拡張の際に問題が発生する場合もあり注意が必要である。また、カスタマイズした部分の権利関係についても利用者と SaaS 提供者間で事前に合意しておくことが必要である。

導入前に適用対象業務における自社の独自性を認識し、導入を検討している SaaS の標準機能とプログラムの改修なしにカスタマイズできる範囲を SaaS 提供者と十分に確認した上で、導入を進めることが重要である。

- **ビジネスに直結する SaaS を導入するケース**

テロや大規模自然災害などの予測困難な事象は除き、SaaS 提供者の設備面や人為的な障害、又は提供者と利用企業間の回線・設備における障害発生時にビジネスが中断あるいは多大な復旧コストや機会損失を招く分野においては、SaaS の導入の是非や障害対策、補償などを慎重に検討すべきである。例えば、給与計算の明細印刷や商品棚卸の際の在庫一覧など、印刷が遅れると業務に支障をきたすものを印刷している途中で、通信障害が発生した場合の印刷中断後の再開オプション（最初から印刷か、障害発生時から再開か）につい

[18] 複数のサーバ、サービスの間でログイン認証情報を共有することで、ID・パスワードを一組ですませる仕組み

ても確認すべきである。

具体的に SaaS を利用できないことによるリスク分析を実施した上で、補償や復旧時間等を SaaS 提供者との SLA に盛り込むことで明確にしておくことが重要である。

- **財務情報、営業機密情報を扱う SaaS を導入するケース**

前述したアカウント情報以上に、情報が不正に閲覧、改ざんされた場合に深刻な影響をもたらすのが財務情報や営業機密情報である。他の分野以上に SaaS 提供者のデータ保護対策について留意する必要がある。

また、財務情報に関しては、必要なときに適切な開示が可能であるか否かが上場企業や上場を検討している企業にとっては重要であるため、事前に確認しておくことが望ましい。

加えて、上場企業が SaaS 型の財務関連のシステムを導入する場合、金融商品取引法の適用を受けるため、次のような要求事項が考えられる。

1. 提供する財務関連のシステムが会計規則等の要件を満たしていることの保障
2. IT 全般統制や財務関連システムの IT 業務処理統制に対する経営者評価や監査人監査への協力を提供者が受け入れることの保障
3. 日本公認会計士協会の監査基準委員会報告書第１８号に準拠した監査報告書の提供

提供者が複数の上場会社に財務関連のシステムを提供している場合、前項に基づき複数の上場企業から経営者評価と監査人監査を受けることになるため、提供者の対応負荷が増大する。これを解決するために、提供者が独立した第三者の監査人から監査を受けた報告書を提供する仕組みとして第１８号に基づく監査がある。当該報告書を複数の上場企業が利用すれば、提供者の対応負荷を削減することが可能となる。

対象分野によっては、SaaS 提供者に預けている情報の漏えいや破損、また何らかの障害で SaaS が利用できなくなった場合に企業に与える影響が大きい場合もある。例えば、中小企業融資制度等で必要な資金融資を受ける場合には決算書が必要であり、特に中小企業においては、財務情報の消失により資金繰りに直結するケースも想定される。しかし、中小企業では自社で十分な IT インフラや体制の用意、あるいは情報セキュリティ対策を実施することが困難であるのも実情であり、そのような場合は、第四章～第六章の SLA の内容等を考慮した上で、信頼できる提供者のサービスを利用し、万が一に備えて保険への加入などリスクの移転をすることで、安心、安全な IT の活用が実現でき、本業に専念できるという点はメリットであろう。

4. SaaS 利用における SLA の重要性

4.1. 現状認識

SLA(Service Level Agreement)は、提供されるサービスの範囲・内容・前提事項を踏まえた上で「サービス品質に対する利用者側の要求水準と提供者側の運営ルールについて明文化したもの」である。サービス利用契約を締結する際に、SaaS 提供者とサービスの利用者（以下、利用者）双方による合意の結果として、契約文書の一部もしくは独立した文書として締結されるケースが多い[19]。

これまで、SLA は、サーバやネットワークといった IT 基盤運用管理サービスの外部委託において利用が進んできた反面、業務用システムについては、ソフトウェア・パッケージを「製品」として利用者が購入し、自ら運用管理を行うことが多かったこともあり、活用範囲が限られていた。しかし、第三者の SaaS 事業者が業務用システムの運用管理を実施し、ネットワーク経由で「サービス」として利用する SaaS では、通常のサービス委託契約と同様に、SaaS 提供者と利用者の間で合意事項を明文化しておくことが肝要である。

SaaS には前述したように利用者の期待が高く、中小企業を含めた企業において、多くのメリットが想定されるため、近年注目・関心が高まっている。その一方で、同時に、以下のような懸念の声も聞かれるようになっている。

- システムの応答速度（パフォーマンス）が遅いのではないか
- システムの調整／変更（カスタマイズ）が自由にできないのではないか
- 既存のシステムとの連携／統合が難しいのではないか
- サービス提供者からのサポートが十分受けられるか
- データのセキュリティが保たれるか不安がある　　等

実際に、これまでは、パッケージ・ソフトウェアをベースとした業務用システムと比較して、SaaS が上記に挙げられているような課題を抱えていた側面は否めない。しかし、関連技術の進歩および SaaS 提供者の努力により、全体的な傾向としてはこれら懸念の多くが解消される方向にある。

このような過渡的な状況においては、利用者の要求水準（期待）と、SaaS 提供者のサービス内容（現実）について、双方の認識が異なることが往々にして起こりがちである。その結果、利用者の過度な期待や幻滅を招くのみならず、トラブルへと発展する恐れがある。

SaaS 提供者および利用者双方にとって様々な可能性を秘めた SaaS の活用促進に向けて、適切な SLA の締結が重要となっている。なお、SLA は締結したら終わりではなく、定めたサービスレベルを定期的に測定、分析、評価することにより継続的にサービス改善を実現

[19] SLA は必ずしも独立した文書として締結されるわけではなく、後述する「努力目標型」の SLA の場合、例えば、SLA を利用者向けホームページ上に公開するにとどまり、未達成時の補償を明確に規定していないこともある。

することも必要となる。こうした管理手法又は運営の仕組み（ルール、プロセス、体制）のことを SLM（Service Level Management：サービスレベル管理）と呼ぶが、SLM を含めた SLA の運用については 5.3 章「SLM の概要」で触れることとする。

しかし、情報システム部門を持たない中小企業においては、後述するような個別の SLA 策定や継続的な SLM の実施が困難であるのが実情であろう。この場合、一般的には SaaS 提供者が予め用意している標準的な SLA を締結することになるが、第六章の確認事項や別表のサービスレベル項目のモデルケース等を参考にして、提供サービスの品質や保証条件を十分に確認するとともに、SaaS 提供者が公開するサービスレベルの運用報告内容や報告頻度についても考慮することが重要である。

4.2. SLA のメリット

前述したとおり、サービス提供における不透明さを解消し、適正なサービスレベルの維持・管理を実現する上で、SLA の活用が有効である。SLA による、サービスの範囲・内容・前提事項およびサービスレベルへの要求水準の明確化と共通認識の形成を通じ、具体的には、利用者および SaaS 提供者双方にとって、以下のようなメリットがもたらされる。

◆利用者におけるメリット（例）

- サービスレベルに対する保証の確保
- サービスレベルが達成されない場合の補償対応の明確化
- 継続的管理によるサービスレベルの維持・向上
- SaaS 提供者選定における判断基準の明確化

◆SaaS 提供者におけるメリット（例）

- サービスに対する信頼性の確保
- サービス提供における責任範囲の明確化
- 利用者との関係維持・強化
- 優れたサービスレベルの提示による競争優位性の確保

SLA が浸透することにより、SaaS 業界におけるサービス品質向上および公正・適切な競争が促進され、結果的に利用者と SaaS 提供者双方の保護に繋がることが期待される。

5. SLA の内容

5.1. SLA の設定内容

◆SLA の形式

SLA はサービス利用契約書の附属資料として添付されることが一般的である。この場合、契約書（本文）に、件名、金額、期間、契約条項などの基本的な契約内容が盛り込まれる。詳細な契約内容を記述した附属資料の中に、SLA が併せて記述されることが多い。

SLA は一般的に以下の要素から構成される。

SLA 構成要素	構成要素の概要
前提条件	サービスレベルに影響を及ぼす業務上／システム上の前提条件
委託範囲	合意された委託内容がカバーする範囲
役割と責任	利用者と SaaS 提供者の役割と責任を明確化した分担表
サービスレベル項目	管理対象となるサービス別に設定される評価項目および要求水準
結果対応	サービスレベルが達成されなかった場合の対応方法（補償）
運営ルール	利用者と SaaS 提供者間のコミュニケーション（報告・連絡）のルール／体制

表 2　SLA の構成要素

なお、前提条件、委託範囲、役割と責任については、通常、契約書に記述されるが、その内容を補完する事項がある場合のみ、SLA にも補足事項が記載される。

◆サービスレベル項目について

SaaS におけるサービスレベルを評価するための客観的かつ測定可能なサービスレベル項目として、下記４分類に関して幾つかの項目が挙げられる。本ガイドラインで示すサービスレベル項目は、SaaS で一般的に必要と考えられる項目が挙げられているが、利用者と SaaS 提供者双方の必要に応じて、既存の SLA ガイドライン等を参考にしながら、追加項目の検討も行う。

分類	項目の概要
アプリケーション運用	システムの使い勝手に関わる項目（可用性／信頼性／性能／拡張性）
サポート	障害対応や一般的問合せ対応に関わる項目
データ管理	データバックアップを含む利用者データの保証に関わる項目
セキュリティ	公的認証や第三者評価（監査）を含むセキュリティに関わる項目

表 3　SaaS のためのサービスレベル項目

サービスレベルの各項目の内容／測定単位／設定例については、附属の別表で詳述する。また、第五章では、SaaS を利用する上で、主に情報セキュリティの観点から確認するべき事項について記述する。

附属の別表においては、SaaS 利用にあたって考慮が必要と想定されるサービスレベル項目と設定例を示す。ここで示す設定例は、現在 SaaS サービスを提供している事業者約４０社（約８０事例）へのアンケート調査を元にまとめたものであり、SLA 作成の際に一般的なモデルケース[20]として活用されたい。実際には、それぞれのサービスレベル項目に対し、業務上の必要性／重要性とのバランスを考慮しながら適切な要求水準を設定することが求められる。

◆SLA 導入の進め方

SLA 導入にあたっては、前述した SLA の構成要素に沿って以下のようなステップを踏むことが一般的である。

①SLA の作成

（ア）前提条件の整理	利用者側の前提条件（業務量、利用者数、等）の洗い出し
（イ）委託内容／範囲の定義	業務要件に基づくサービス内容／範囲の決定
（ウ）役割／責任分担の定義	利用者と SaaS 提供者の作業分担の明確化
（エ）SaaS 提供者の免責範囲の定義	SaaS 提供者の免責事項の検討（利用者の過失／故意による障害、等）
（オ）サービスレベルの定義	具体的なサービスレベル項目の設定、測定方法の検討および目標保証型サービスレベル・努力目標型サービスレベルの設定
（カ）結果対応の定義	サービスレベル未達成時の対応手順および補償の検討
（キ）運営ルールの設定	運用段階におけるコミュニケーション（報告・連絡）ルールの設定

なお、SaaS 提供者が予め標準的な SLA を用意している場合は、その SLA で上記内容が明確になっているかどうかを確認し、不明瞭な場合は SaaS 提供者と利用者で十分に協議を行うこと[21]。

また、SaaS 提供者は、SLA について利用者が容易に理解できる表現を用い、可能な限

[20] 本モデルケースで示す設定例を参考として、実際の設定値は、業務内容など個々の状況に応じて決定されるべきものである点に十分に留意されたい。

[21] ただし、マルチテナントの場合は協議を行ったとしても、必ずしも利用者側の要求事項が実現できるわけではない。

り専門用語を使用しないこと。

②SLA の締結

SLA 仕様書への必要事項の記載および SaaS 提供者への提示、あるいは標準的な SLA 仕様書の記載内容に合意し、SLA を締結する。

③SLA に基づく管理

SLA は締結後の運営・管理が重要となる。そのための手法又は運営の仕組みである SLM（Service Level Management：サービスレベル管理）の進め方と注意点は、「5.3. SLM の概要」で述べる。

◆利用者／提供者の役割分担（責任範囲）

SaaS の導入にあたっては、SLA では担保されない様々な作業が必要となる。利用者と SaaS 提供者がそれぞれどのような役割を負いどのように分担するのかについて、個々の作業と役割分担を明確化しておくことが求められる。アプリケーション運用、サポート、データ管理、セキュリティといった SLA 上に明記するサービスレベル項目以外に検討が必要な主な項目としては、データ移行、アプリケーション導入、既存システムとの連携、教育・トレーニングといった作業が挙げられる。SaaS の場合、基本的には利用者が自らこうした作業を行う必要があるが、SaaS 提供者が有償・無償の支援サービスを用意しているケースが多いため、予め予想される作業を洗い出し、利用者と SaaS 提供者の役割分担表を作成しておくことが望ましい。

5.2. サービスレベルの定義

SLA 作成にあたっては、サービスレベルの定義が最も重要な作業となる。具体的には、サービスレベル測定のための項目を設定し、各項目が満たすべき水準を、測定可能な形で決定する。対象となるサービスと要求水準の設定にあたっては、万一トラブルが発生した場合に業務に与える影響を考慮した上で優先順位を見極め、重要度が高いものを中心に定義を行う。多くの項目を設定することも可能だが、管理負荷の増大やコスト上昇を招く場合があるため、必要なものを吟味し、絞り込むことが重要である。

また、サービスレベルを決定する際には、利用者と SaaS 提供者の間で認識の相違が起こらないように、客観的な項目（定量的な数値、数式による測定等）を定めることがポイントとなる。

5.3. SLM の概要

SLM とは、サービスに関わるルール、プロセス、体制等の改善により高品質なサービスを維持し、サービスレベルの要求水準とサービス内容を利用者の事業上の要求の変化に対応させるための継続的な運営・管理手法である。SLM においては、利用者と SaaS 提供者が協力して問題を確認し、根本原因の分析やプロセスの変更等を通じて問題再発を防ぐ継続的な問題解決が重要となる。

SLM の進め方

通常、SLM においては以下のようなステップを踏む。

① 測定　サービスレベルに基づくサービス内容の測定
　①-1：データの収集　関連データの収集
　①-2：データの比較　測定結果と要求水準の比較
　①-3：結果の報告　利用者と SaaS 提供者双方の関係者への報告／連絡
② 分析・評価　問題の識別／優先度の判断／改善機会の確認
　②-1：結果の識別　最も深刻な問題の特定と優先順位付け
　②-2：根本原因の分析　問題を引き起こしている原因の特定
③ 改善　問題箇所（機能、ルール、プロセス、体制等）の修正
　③-1：解決策の作成　優先順位の高い問題に対する解決策の検討
　③-2：解決策の合意　関係者による解決策の承認
　③-3：解決策の実施　合意された解決策の展開
④ 報告・連絡　達成された効果を維持するための継続的コミュニケーション
　④-1：監視　変更後の定期的な監視
　④-2：フォローアップ　改善効果と新たに明確になった課題の関係者への伝達
　④-3：フィードバック　サービスレベル更新が必要な場合の報告

結果対応

目標保証型サービスレベル未達成の場合の結果対応としては、主に運用上／財務上／契約上の対応が考えられる。

- 運用上の対応　リソースの増強や代替手段の適用
- 財務上の対応　金銭的な補償の設定
- 契約上の対応　中途契約解除条件の設定

いずれも、業務への影響／緊急性／重要性を踏まえて具体的な内容を定義することになる。財務上の対応については、払い戻しではなく将来の請求額から差し引く形態をとり、

上限を設定することが一般的である（例：月の請求額に対する１０%、１日分の請求額、等）。

また、一般的に結果対応に関する瑕疵担保責任は主契約書上で明記する必要がある。更に、SLA に記載されるサービスレベル項目は、必ずしも全てが目標保証型（保証義務が発生）ではなく、努力目標型（努力目標に留まる）として設定されるものもある。努力目標型の場合は補償が明確に規定されないが、その分弾力的な運用が可能となる。

なお、自然災害、電力供給の停止、通信遮断等のインフラ障害や、利用者側の問題に起因する事由によって要求水準を達成できない場合を想定して、SLA の適用対象外となる免責事項が設定されるのが通例である。

運営ルール

SLA は契約書の附属資料として締結されることが一般的であり、実際の業務に即して定期的に見直し・変更を行うことが望ましい（例：月次あるいは四半期単位で微修正を行い、年次単位での公式的な見直し・変更を行う等）。

また、SLA 導入／定着にあたっては、現実的な水準値に落とし込むまでに相応の試行錯誤期間を要する点に注意が必要である。そのため、SLM の実施においては、SLA 運営組織を立ち上げ、利用者と SaaS 提供者双方で SLA 項目の変更、設定値の変更プロセスを含む運営ルール（責任者、報告・連絡経路、等）を明確化しておくことが求められる。

SLM の成功には、計画段階からの利用部門（エンドユーザ）の参画が必須であるため、SLM 運営組織を立ち上げる際には利用部門の主要関係者を配置し、SLA／SLM の重要性について早期に共通認識を形成することが肝要となる。

6. SaaS 利用における情報セキュリティを中心とした SLA 上の確認事項

情報セキュリティの基本的な考え方に、機密性、完全性、可用性[22]がある。更に、昨今は内部統制上の要求から、説明責任、追跡可能性（トレーサビリティ）[23]等も求められるようになりつつある。SaaS を利用する上でもこれらの要求事項に対して、正しい実装や運用を行わなければならない。本章では、SaaS 提供者選択に関する SLA 上の要件を、特に情報セキュリティの観点から考察し、利用者が確認すべき事項を列挙する。

なお、要件の考察に際しては、情報セキュリティ監査等で確認されるべき事項の単なる繰り返しにならないよう、特に重要と考えられる要件、つまり、SaaS であること、データを外部事業者に預託し、ネットワーク経由でウェブアプリケーションの提供を受ける、という性質が孕むリスクを低減するための要件について考察の対象としている。

また、一般的には高いレベルの SLA を設定する場合、サービス価格も高くなることを理解しておく必要がある。例えば、メンテナンスのために計画的に停止することが可能なシステムと２４時間３６５日絶対に停止しないシステムでは運用コストが大きく異なる。利用するアプリケーションや利用者のビジネスに必要な条件で、最適なサービスレベルを選択するべきである。

6.1. 各種セキュリティ規格の準拠性に関する確認事項

SaaS 提供者選択に際しては、安全性検証の観点から、JIS Q 27001:2006（ISO/IEC 27001:2005）[24]の要求事項を基本としたセキュリティ対策の実施状況を確認することが重要である。更に、ウェブアプリケーションの脆弱性検査、サイトのペネトレーションテスト[25]（又は検査）等、第三者による安全性検証試験／セキュリティ診断を定期的に実施し、結果を顧客に対して公開していることを前提条件として考えるべきといえる[26]。顧客のデータを預かり、運用する事業者としては常識の範疇と考えることができ、また、サービスの継続性、信頼性の高さを判断する基準ともなる。また、プライバシーマーク付与認定、ISMS 認証取得、情報セキュリティ監査制度の利用等を行っている企業においては、必要に応じて利用者企業の基準に応じた監査を行うことができるかどうかも重要な判断要素となる。

各 SaaS 提供者に対して、これらの検証試験の実施状況と結果の閲覧を要求し、安全性が検証されていることを確認することが重要である。もしも、合理的な理由がないのにもかかわらず試験を実施していない場合には、試験の実施を要求する、あるいは、その SaaS 提

---

[22] セキュリティの代表的な三要素。それぞれ、情報の秘匿性、情報が不正に変更されていないことを各自にすること、情報が必要な時に使用できる状態にあること、を意味する。

[23] 情報の正確性を検証するため、情報の作成、編集、閲覧、消去といったイベント発生に関するデータ（ユーザ、発生日時等）を保管管理しておくこと。

[24] 情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項

[25] 既知の脆弱性を悪用した攻撃を実際に行う、侵入可能性試験のこと

[26] 第三者による安全性検証試験／セキュリティ診断の検証レベルは様々であり、自社のサービスレベルに必要な検証内容であるかを確認するとともに、一般的には検証レベルが高度になれば SaaS 利用料金も高くなる点にも留意されたい。

供者を選択することは避けるべきである。

また、SaaS 提供者のサービスはソフトウェアの機能のみを提供しているのではなく、その利用におけるサポートも重要なサービスの一つになる。このような観点から、IT サービスマネジメントが正しく実行されていることも、SaaS 提供者選択の重要なポイントになるだろう。ヘルプデスクの設置や迅速なトラブル対応などの体制や仕組みなどについては、IT サービスマネジメントのベストプラクティスである ITIL に取り組んでいるか、また JIS Q 20000:2007 認証を取得しているかなどについても確認を行うことが望まれる。

6.2. 機密性に関する確認事項

SaaS ではその特性から多くの情報が他社と同様のデータベースで管理されている。したがって、データベースシステムが本来持っているセキュリティ上の懸念事項についてはそのまま自社の情報管理体制へ引き継がれることになる。SaaS 提供者でも十分な対策を実施していると考えられるが、提供者選定時には脆弱性や脅威に対する対策の状況について確認することが重要である。例えば、使われているデータベースシステムの種別、バージョン、セキュリティパッチの適用ポリシー、システム構成等について決められた範囲で確認を行い、必要なセキュリティ対策が講じられていることを確認すること。

また、データベースシステムだけでなく、データベースに蓄積されているデータの種類や特性についても確認をしておいたほうが良い。蓄積される情報の種別、情報管理に関するアクセス制御の内容を明確にしておく必要がある。

例えば、企業内において、職種別に情報へのアクセス権を細かく管理しているとしても、利用するサービスによっては、利用者企業で実施しているレベルまで情報や職種を細かく分類していないために、自社が行っている実施レベルよりも大まかな管理になってしまうという場合も考えられる。つまり、自社の管理レベルが部長には閲覧を許すが課長には許していないといった場合でも利用するサービスが管理職という分類しかなければ、部長でも課長でも閲覧が可能となってしまう。個人情報などのように、氏名、住所などの単独の要素だけではなく、いくつかの要素が同時に閲覧できることで価値やリスクが変化するような情報の取扱においては、厳格な情報管理が難しくなる可能性がある。

あるデータについて社内規定によれば「管理者は入力できるが、一般社員は閲覧しかできない」とされている場合に、SaaS で提供されているユーザ権限が十分に対応できないことがあるだろう。情報統制という観点からみれば、機能不足という判断になってしまう。内部統制に関わるコンプライアンス構築の一環として業務分掌を作成している企業も多いが、その粒度と SaaS 提供者が提供する利用者権限機能が合致していないことで発生するリスクについても考慮しておかなければならない。

この他に、ネットワーク、特にインターネット上でデータをやりとりすることが要因となる情報漏えいリスクは大きい。ウェブアプリケーションの場合の通信は HTTP 又は

HTTPS[27]で行われる。HTTP では機密性は提供されないため、SaaS 事業者との通信は HTTPS を用いることが要求される。また、HTTPS 利用と比べより費用はかかるが、暗号化をサポートした VPN[28]を利用することで、第三者に対する機密性の保証は高まる。しかし、通信路の保護だけでは十分ではなく、預託データを記録したハードディスク、光学メディア、USB メモリなどの記憶媒体の管理状態やデータベースへの直接アクセスによる情報漏えいを防ぐための適切なアカウント管理等、データ保護の管理策についても確認する必要がある。

また、ウェブアプリケーションに脆弱性が存在すると、第三者による不正アクセスによってデータが漏えいする可能性があるため、SaaS 提供者が提供するウェブアプリケーションに脆弱性が存在しないこと、正確には、既知の調査手法で発見される脆弱性が存在しないことを確認するための検査の定期的な実施と結果の報告を求めることが重要である。

6.3. 完全性に関する確認事項

データが漏えいしなくとも改ざんされることで業務の信頼性が損なわれる、また、消去されることで業務が継続できなくなる等、重大な問題が発生する場合があるため、預託データの完全性、整合性検証について対策が施されていることを確認することが重要である。

また、アプリケーションにおいて、入力データの妥当性の検証機能が実装されていることを確認することが重要であり、正しく記録（ログ）がとられているかどうかも重要なポイントとなる。

情報システムを効果的に活用するには蓄積したデータの再利用が不可欠である。SaaS は提供者のデータベースにすべてのデータが蓄積されており、これを自分用に加工したり、編集したり、修正して出力するためには一度利用者の手元にダウンロードするなどの作業が必要になる。もしもダウンロードができないのであれば、必要に応じてデータの加工ができるツールなどが提供されていなければならない。

ダウンロードしたデータが特別な形式のものでは再利用できないため、標準的なフォーマット、カンマ区切り、タブ区切り、XML[29]、テキスト等の一般的なデータ形式でダウンロードが可能であることを確認することが重要である。

なお、データをダウンロードした場合は SaaS 上で確保されていたデータのアクセス管理が解除されることになる。多くの場合、ダウンロードしたデータには「社外秘」、「取扱注意」などのラベルが記載されないため、あらためて情報管理規定を遵守した形での分類が必要となることに注意すべきである。

また、SaaS を解約する際にデータを引き取ることができるのかについても重要なポイントになる。これまでに入力したデータが消失してしまっては業務の継続が困難になってしまうため、契約時から解約する際の権利関係について確認をしておく必要がある。

---

[27] HyperText Transfer Protocol Security
[28] Virtual Private Network、仮想的な閉域ネットワークを設ける技術
[29] eXtensible Markup Language、文書やデータの意味や構造を記述するためのマークアップ言語の一つ

6.4. 可用性に関する確認事項

SaaS は従来の ASP のようにアプリケーションそのものを提供することもあれば、アプリケーションの一部として利用されることもある。双方の場合においても利用したいときに正しく利用できるかどうかが重要なポイントとなる。

また、SaaS の特徴として柔軟なカスタマイズ機能や、マッシュアップ[30]による機能の融合などがある。この際に期待していた処理が実施されているか、データの受け渡しは適切か等の正確性についても十分に確認する必要があるだろう。このようにマッシュアップ等で複数の SaaS を連携した複合型サービスを利用する場合、それぞれの役割と責任範囲を明確にしておくことが望ましい。

SaaS では、サービスは使いたいときにいつでも利用できる状態になっていなければならず、必要に応じてサポートを受けられるようになっていなければならない。IT 活用における稼働率という観点でとらえれば、ITIL[31]を活用した SLM をベースに実施するというのも良い方法である。SaaS 提供者との契約においては、SLA を締結することで責任の区分も明確になるだろう。

サービス継続性については、災害時、障害時にどの程度システムが停止する可能性があるのかを明確にしておく必要がある。SaaS のサービスそのものがネットワークさえ通じていれば提供できるという利便性がある反面、コスト削減などを目的に、国内外を問わずサービス継続性の低いデータセンタなどに設置された場合にサービスの停止だけではなく、復旧に要する時間も特定できないという問題が発生する可能性がある。

また、トラブル時だけではなく、様々な問題や要求事項について迅速な対応をしてもらえるのかどうかも重要なポイントになるだろう。例えば、国外の SaaS 提供者で国内拠点がないというような場合に電話や電子メールでのサポートに時間を要する、また、質問そのものを英語などの外国語で行わなければいけないなど、更に大きな負担となることも想定される。

6.5. 運用保守における確認事項

どのようなシステムであっても保守のためのシステム停止は避けることができない。システムの多重化により保守作業による停止時間を見かけ上、ゼロにすることは可能であるが、利用者全員の合意がとれる程度のシステム規模であれば、一斉にサービスを停止して保守作業を実施することでコストを低減することも可能である。いずれにせよ SaaS 提供者が保守計画を管理していることを確認することが重要である。

SaaS では人事や給与、経理に関するサービス等も提供されている。労務管理、給与管理、

---

[30] ウェブ上に提供されているコンテンツやサービスを組み合わせて、新しいサービスを形作ること。地図上にお店などの情報を表示するサービスが有名。

[31] Information Technology Infrastructure Library、IT サービスマネジメントにおけるベストプラクティス

会計管理については、最新の法制度（商法、会社法、税法、労働法等）に適合出来る体制が構築されているかどうかについても確認しなければならない。会計に関するサービスを提供している提供者が、法令改正後にアプリケーションのアップデートをしていないとすれば、SaaS から得られるアウトプットは要求される要件を満たしていないデータや帳票になる可能性がある。法令対応をしていないデータをダウンロードして加工することは、対応させるための追加的な作業を発生させるため、情報システムを効果的に利用しているとは言えないだろう。

SaaS 提供者選択において盲点となりがちなのは国内法令対応である。SaaS においては単に価格やサービス内容で提供者を選択してしまうことも想定されるが、ビジネスにおいて法令等の遵守は基本的な要素であり欠くことは許されない。国内法令に対応していない SaaS 提供者の採用は業務を複雑にするばかりでなく、データ保全、説明責任という観点からも事故を発生させやすいということを認識する必要がある。海外のサービス提供者の場合は特に、これまでの法令改正における対応の迅速さや、今後の計画などについて、契約前に情報収集をしておくことが望ましい。

SaaS を利用している際に発生したトラブルのすべてを提供者の責任にすることは現実的ではないため、必要に応じてトラブル対応を利用者側で行うことも想定しておくべきであろう。自社所有システムであればトラブルの原因分析に必要な記録をすべて残しておくことが可能だが、SaaS として提供されている場合、提供者が想定している内容での記録のみになってしまう可能性が高い。必要な記録がその中にすべて含まれていれば問題はないが、そうでなければ障害が発生しているかどうかも判断することができない可能性がある。何がトラブルなのか、セキュリティ障害なのかの判断基準は企業によって様々であり、事業影響度分析（BIA[32]）やリスクアセスメントに基づいて決定されている。なんらかの軽微な事象、例えばファイルの一部廃棄等の事象が発生した場合に、SaaS 提供者の基準では「報告の必要なし」と判断されるかもしれないが、利用者側の基準では「報告の必要あり」と判断すべきものもあるかもしれない。その事象を許容するかどうかは利用者側の事業影響度分析やリスクアセスメント[33]の結果に沿うものであるべきであろう。

このように、利用者が求めているすべてについて SaaS 提供者が対応できるとは限らないため、それを前提に提供者の責任と利用者の責任を明確にし、SLA に反映させておかなければならない。そのためには利用者側に「何をもって報告すべき事象とみなすのか」について明確な基準を決めておくことが必要である。

また、SaaS 提供者で障害が発生する可能性はゼロではない。利用者の事業に対する事業影響度を勘案した上で提供者の責任を明確にしておかなければならない。契約書や SLA に基づいて対応をしてもらうことになるが、どのような対応をした場合でも報告書をもらう方が有益であるため、契約書や SLA に報告書提出に関する項目があるかを確認することが

[32] Business Impact Analysis
[33] あるイベント・リスクが業務に与える影響を分析すること。

重要である。

6.6. コンプライアンス対応における考慮事項

金融商品取引法、会社法に関連して内部統制上の説明責任について明確にすることが求められている。情報システムにおける説明責任についてはログの保全が挙げられることが多いが、本質的には ID 管理とログの保全、事象（イベント）管理の 3 点が行われていなければ十分ではない。

まず、ID 管理においては「一人の利用者につき一つの ID を付与すること」が原則となる。説明責任においては誰がいつ何をしたのかを明確にしなければならない。ある情報システムにおいて、複数の者が一つの ID を共同利用していた場合にある事象を誰が起こしたのかについて判別が不可能なため、明確な説明を行うことができない。このように ID の付与に対して原則を守っていないと、内部統制上の説明責任を果たせないことになってしまう。SaaS 提供者に対しては、個人に付与した ID がログの検索に利用できることを確認することが重要である。

次にログの保全については、従業員の行動管理という意味で一定期間保管することが原則となる。行動記録は、何かの事象が発生した際に行為者を見つけ出すために利用するものと思われていることが多いが、それだけではなく、従業員が不正行為を行っていないことの証明にも利用されうるものでもある。したがって、違反行為だけではなく、正しい行為を証明することについても記録をしておかなければならない。しかし、すべての行動を記録することはログのデータ量が膨大になってしまう可能性があるため、どの種類のログを、どの程度の期間、記録しておけば良いのかを事前に決めておくことが望ましい。

事象管理については、すでに説明した通りである。何が違反なのか、何がトラブルなのかを明確にし、早期発見することによってトラブルの影響を少なくすることができるばかりでなく、経営者による状況の把握などにも有益である。

6.7. 確認事項一覧

ここまでに論じた確認事項、具体的な確認ポイントについて以下にまとめる。

(1) 安全性検証試験の実施と結果の確認

第三者による以下の安全性検証試験および認証の更新を定期的に実施していることを確認し、サービス導入前に監査結果、検査結果、試験結果を確認すること。特に、従業員（派遣従業員等、第三者を含む）のセキュリティ教育状況を確認し、預託データの取扱に十分な配慮がされているかを検証すること。

- JIS Q 27001:2006、JIS Q 27002:2006 **に基づくセキュリティ監査、システム監査**
- **ペネトレーションテスト等ネットワークからの攻撃に対する検証試験**
- **ウェブアプリケーションの脆弱性検査**
- **データベースセキュリティ監査**
- **プライバシーマーク付与認定**
- ISMS **認証**

検証試験が標準化、規格化されていない分野では、SaaS 提供者自身で監査を行っていることも考えられる。その場合は、監査報告書を第三者のセキュリティ専門家に確認してもらうことが望ましい。

(2) データおよびデータベース管理

- **データベースに蓄積される情報はどのようなものか整理されているか**

アカウント情報や顧客情報といった個人情報、営業情報、財務情報等の機密情報等、データベース中のデータを分類し、整理しておくこと。

- **預託データの整合性検証作業が実施されていること**

入力データ、算出データ等がアプリケーションの問題や不正な操作により改ざんされていないことを検証する手法が実装され、検証報告の確認作業が行われていること。

- **入力データの妥当性検証機能が実装されていること**

金額、住所、電話番号等の文字種、データ形式が制限されるフォームにおいて、想定外のデータ入力を検出し、不正なデータをデータベースに格納しないようにする仕組みを提供していること。

- **預託データのダウンロードが可能であること**

セキュリティの観点からは、SaaS 提供者だけでなく利用者側でもバックアップを実施しておく必要がある。ただし、SaaS 提供者は十分にシステムの信頼性対策、サービス継続性対策を行っていると考えられるが、トラブル時に備えて、預託データのダウンロードが可能かどうかを確認すること。

- **ハードディスク、光学メディア、**USB **メモリ等、二次記憶媒体の安全性対策が実施されていること**

バックアップメディア等では権限のあるものだけにアクセスを限定し、廃棄の際にはデ

ータの完全な抹消を実施・検証、USB ポートを無効化しデータの吸い出しの制限等の対策を講じていること。

(3) アカウントおよび ID 管理

- **情報に対するアクセス権限を利用者ごとに設定できること**

利用者組織にて規定しているアクセス制限と同等な制約が実現できるかどうかを確認すること。SaaS アプリケーションで用意されているロール（管理者、一般ユーザ等の役割を意味する）に制約がある場合には、ユーザを既存のロールの範囲でグルーピングする等の工夫により対応できるかどうかを確認する。SaaS ではマルチテナントを採用しているため、他の顧客と一つのデータベースを共有する場合があることに配慮すること。

- **利用者個人毎に ID を発行していること**

利用者側で共有アカウントを設けなければ、利用者毎に異なる ID が発行されていると考えられるが、ログ上でデータ操作ユーザを識別するためにも利用者個人毎に ID を発行していることを確認しておくことが望まれる。

(4) ログ管理

- **操作ログ上で利用者個人の ID が付与されていること**

アプリケーションサーバ上で取得できるログには、大きく分けて、ウェブサーバが生成するログ（HTTP レベルのリクエストおよびレスポンス）、データベースが生成するログ（接続および解放、SQL クエリおよびレスポンス、データ操作、特権ユーザ実行コマンド等）、アプリケーションが生成するログがある。利用者側で必要となるログは主にアプリケーションサーバ上で取得できるログであり、そのログ形式は SaaS 提供者の実装に依存する。利用者にとって必要な情報は、誰が、いつ、どのデータに対して、どのような操作をしたのか、ということであるが、重要なことはログに記される「誰が」の部分であり、この部分に、利用者各人の ID が記されることを確認する。

- **取得するログの種類、期間を指定できること**

SaaS 提供者ではログを大量に保管しているため、具体的なログの指定をせずに単にログを要求しただけでは膨大な量の受け渡しが必要となる。必要なログを、アプリケーションの機能、表示されるページの URL 等の区分と、月、週、日、時間等の任意の期間の組で指定できることを確認する。

- **利用者側の基準に応じた判断ができるためのログを提供できること**

SaaS 提供者と利用者においては、何をもって障害又は事故と見なすかの判断基準は異な

ることが予想される。サービス利用開始前に自社の判断基準の比較を行い、利用者側が厳しい基準を持つ部分等両者に差異のある部分においては、その差異を解消するため、ログを提供者から提供して判断を委ねるような体制を整えておくこと。

(5) 保守およびサポート

- **保守計画を管理し提示していること**

SaaS ではアプリケーションとデータの双方を預託しているため、SaaS 提供者の保守作業によりサービスが停止してしまうとデータにアクセスすること自体ができなくなる。共同利用という SaaS の性格上、サービスの停止に至ることは少ないと考えられるが、提供者におけるメンテナンス作業計画について提示を求め、計画の内容について利用者の事業計画上、障害となることが無いことを確認すること。

- **サポート時間について利用者組織の業務時間と合致していること**

オンラインアプリケーションサービスという性格上、ほとんどの提供者は２４時間３６５日のサポート体制を構築していることが多いが、SaaS 提供者によってはシステムおよびサポートデスクを国外に設置し、日本時間における９時から１７時の間に、電子メールおよび FAX のみの対応となっているかもしれない。迅速なサポートを受けるため、利用者の業務時間中は電子メールおよび FAX での対応に加えて電話においてもサポートが受けられることを確認すること。

- **最大停止時間の提示と事故の可能性評価に対する報告があること**

SaaS 提供者において万全を期していても障害によるサービス停止の可能性を否定することはできない。想定される障害毎の最大停止時間と推定障害発生確率の提示を求め、自身の事業継続計画に反映させることが重要である。

(6) その他の管理策

- **HTTPS 又は VPN による通信路の保護が可能であること**

ユーザ認証時のみならず、認証後の通信は HTTPS 又は VPN 等により機密性と完全性の保証がされていること。なお、SSL が使用される場合には SSL 3.0 および TLS 1.0 に限定し、脆弱性のある SSL 2.0 は使用しないこと。

- **国内法令等の改正に対応したアプリケーションのアップデートが計画・実施されていること**

サービスアプリケーションに関わる法令等の洗い出し、改正時期の見積り、対応計画の策定等の実施について確認すること。

- **利用者による情報セキュリティ監査を受け入れていること**

SaaS 提供者が実施した情報セキュリティ監査報告書は必ず確認する。加えて、預託するデータの重要性に応じて、サーバ設置環境（データセンター等）の確認、利用者による第三者セキュリティ監査の実施等を SaaS 提供者が対応可能であることを確認する。

- **事業影響度分析やリスクアセスメントを前提とした SLA を締結すること**

SaaS 提供者と SLA 条項を定める際には、想定される事象が事業に与える影響やリスクの評価を行い、何を以てトラブルとみなすかの判断基準を明確にしておくこと。

- **適切な個人情報取扱事業者保険に加入していること**

アプリケーションで個人情報を扱う場合には、SaaS 提供者との間で個人情報取り扱いに関して合意を形成して契約事項の中で責任の割り当てを行っておくべきであるが、万が一の個人情報漏えいに備える意味で SaaS 提供者における損害賠償保険加入の有無を確認しておくことが望ましい。

7. SaaS を効果的に利用するための利用者側の留意事項

これまでは SaaS 提供者選択の観点を列挙してきたが、SaaS をより効果的に利用するためには利用者側でも十分な準備を要する。最初に当該サービスの導入に当たり利用企業は経営改革や業務改善についての検討と準備を行い、提供されるサービス機能が自社の経営の成熟度を考慮して必要十分なサービス内容であるかを検討する必要がある。また、提案される SLA は経営改革や業務改善など自社のビジネスを強化するために必要十分なサービスレベルであるかを経営面から検証を行うことが望ましい。検討に当たっては、IT ベンダ、IT コーディネータ等の外部専門家を活用し客観的な評価を行うことも有効な手段である。

IT 環境に関して、最初に準備、確認すべきはネットワーク環境の整備状態である。SaaS を利用するためには、高速かつ安定したインターネット接続環境が必要になる。利用者側は、自社の利用量に見合った通信回線能力について検討し準備しなければならない。更に、利用者側のローカルエリアネットワークについても十分な帯域が確保されていなければならない。

次に確認するのはシステム環境である。常識的なことであるが、各利用者の端末にウェブブラウザがインストールされていること、最新のバージョンであることを確認する。注意すべきポイントとして、SaaS 提供者の提供するサービスによってはウェブブラウザのプラグインを利用する等の理由で、正常にサービスを受けることの出来るウェブブラウザが限定されている、又は指定されている場合がある。利用者各人の OS の種類、バージョン、利用するウェブブラウザの一覧表を作り、SaaS 提供者のサポートしていない環境が使われていないことを確認する。

また、各使用者に対してウェブブラウザの利用における一般的な脅威や脆弱性に対する教育などを予め行っておく重要である。昨今、Winny 等による情報漏えい事件が後を絶たない現状では、利用者全員に対して、オープンなインターネットを活用するリスクを周知徹底する情報モラル教育への取組が必須である。また、社内の SaaS 利用者が SaaS システムへの攻撃、あるいは同一 SaaS システム上の他社利用者をターゲットにしたクラッキング[34]行為の可能性もあり、不正利用を防止する情報モラル教育への取組も重要である。

ウェブアプリケーションの特色についても確認しておかなければならない。例えば、データ入力においては「送信」ボタンを押すまでは入力内容が反映されないことや、アプリケーションによってはウェブブラウザ標準の「戻る」ボタンをクリックすることで、セッションが切れてしまうといったトラブルが発生する可能性がある。

更に、トラブル時の問い合わせ先や、トラブルの判断基準なども明確にしておくことで、サービスの継続性に貢献するだろう。

最後に、業務プロセスにおけるサービスの重要性について、リスク分析や事業影響度分析が実施されているかを確認する。SaaS 提供者がいくら良いベンダであっても、自社のサ

[34] 不正な意図を持ってシステムを利用しようとする行為。

ービスレベルと合っていなければ、ビジネスに利用することはできないため、必要に応じて外部専門家を活用しながら、利用者がサービスレベルについて項目別に検討し、SaaS 導入の準備をすることが重要である。また、自社の業務における IT サービスの最大許容停止時間を明確にしておくことで、万が一のトラブル時への備えができ、最大限に SaaS を利用することができるだろう。

以上

参考文献

- 民間向けの IT システムの SLA ガイドライン第三版（社団法人 電子情報技術産業協会 ソリューションサービス事業委員会、２００６年１０月）
- IT サービス･リスクマネジメントと SLA　～IT サービスリスクのコントロール手段としての SLA 活用～（社団法人 電子情報技術産業協会 ソリューションサービス事業委員会、２００７年３月）
- 公共 IT におけるアウトソーシングに関するガイドライン（総務省、２００３年３月）
- ASP 公式ガイド（ASPIC、２００１年９月）
- 外部委託における情報セキュリティ対策実施規程策定手引書（内閣官房情報セキュリティセンター、２００６年３月）
- 情報システムに係る政府調達への SLA 導入ガイドライン（独立行政法人情報処理推進機構、２００４年３月）
- 先進的『ウェブ・サービス』を中心とする情報技術ロードマップ策定～ソフトウェアサービス化および情報の高付加価値化への潮流～報告書（IPA ソフトウェア未来技術研究会、２００７年７月）
  （http://www.ipa.go.jp/about/pubcomme/200707/index.html）

謝辞

SaaS 向け SLA ガイドラインの作成にあたり、情報提供および執筆にご協力いただいた独立行政法人情報処理推進機構（IPA）並びに同機構に設置した「SaaS 利用者の観点からのセキュリティ要件検討会」の方々に厚くお礼を申し上げます。

SaaS 利用者の観点からのセキュリティ要件検討会　名簿

座長

大木 栄二郎　工学院大学 情報学部 教授

委員

及川 喜之　株式会社セールスフォース・ドットコム チーフテクノロジーオフィサー
大畑 毅　日本電気株式会社 マーケティング本部 グループマネージャー
大野 祐一　株式会社ラック 研究開発本部 データベースセキュリティ研究所 所長
河野 省二　特定非営利活動法人 日本セキュリティ監査協会 スキル部会副部会長
喜入 博　KPMGビジネスアシュアランス株式会社 顧問
北原 佳郎　ラクラス株式会社 代表取締役社長
駒瀬 彰彦　株式会社アズジェント 取締役 技術本部長 シニアコンサルタント
塩崎 哲夫　富士通株式会社 情報セキュリティセンター長
丸山 宏　日本アイ・ビー・エム株式会社 東京基礎研究所 所長
丸山 満彦　監査法人トーマツ エンタープライズ リスク サービス

別表

SaaS 向け SLA におけるサービスレベル項目のモデルケース

※ 本モデルケースでは、基幹系業務の場合と販売管理やグループウェアなどそれ以外の業務の場合に分けて、サービスレベル設定例を示している。
※ 実際の設定値は、以下の設定例を参考として、業務内容など個々の状況に応じて決定されるべきものである点に留意されたい。

◆アプリケーション運用

種別	サービスレベル項目例	規定内容	測定単位	設定例	備考
可用性	サービス時間	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	24 時間 365 日 （計画停止／定期保守を除く）	計画停止時間は提供者が個々に設定
	計画停止予定通知	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	30 日前にメール／ホームページで通知	
	サービス稼働率	サービスを利用できる確率（(計画サービス時間－停止時間）÷計画サービス時間）	稼働率（%）	99.9%以上（基幹業務） 99%以上（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
	ディザスタリカバリ	災害発生時のシステム復旧／サポート体制	有無	遠隔地のバックアップ用データセンタで保管している日次バックアップデータと予備システムへの切り替え	データセンタ構成、復旧までのプロセス／時間、費用負担についても明示されていることが望ましい また、適用する業務の重要性に応じた「ディザスタリカバリ」のレベルにより設定内容は変わる
	重大障害時の代替手段	早期復旧が不可能な場合の代替措置	有無	バックアップデータの取得が可能なホームページを用意	
	代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	有無（ファイル形式）	CSV あるいは Excel ファイルで提供	
	アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	有無	年 2 回の定期バージョンアップを実施	頻度、事前通知方法、履歴管理／公開、利用者の負担についても明示されていることが望ましい

別表

種別	サービスレベル項目例	規定内容	測定単位	設定例	備考
信頼性	平均復旧時間	障害発生から修理完了までの平均時間（修理時間の和÷故障回数）	時間	1 時間以内（基幹業務） 12 時間以内（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
	システム監視基準	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視	有無	1 日 4 回のハードウェア／ネットワーク／パフォーマンス監視	詳細な監視項目は提供者が個々に設定
	障害通知プロセス	障害発生時の連絡プロセス（通知先／方法／経路）	有無	指定された緊急連絡先にメール／電話で連絡し、併せてホームページで通知	初期対応後の経過報告の方法・タイミングについても明示されていることが望ましい
	障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	時間	15 分以内（基幹業務） 2 時間以内（上記以外）	営業時間内／外で異なる設定を行う場合がある
	障害監視間隔	障害インシデントを収集／集計する時間間隔	時間（分）	1 分以内（基幹業務） 15 分（上記以外）	営業時間内／外で異なる設定を行う場合がある
	サービス提供状況の報告方法／間隔	サービス提供状況を報告する方法／時間間隔	時間	月に一度ホームページ上で公開	報告内容／タイミング／方法は提供者が個々に設定
	ログの取得	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）	有無	セキュリティ（不正アクセス）ログ／バックアップ取得結果ログを利用者の要望に応じて提供	提供内容／方法は提供者が個々に設定
性能	オンライン応答時間	オンライン処理の応答時間	時間（秒）	データセンタ内の平均応答時間 3 秒以内	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
	バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	4 時間以下	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
拡張性	カスタマイズ性	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	有無	利用画面上の項目配置変更や新規項目の追加が設定画面より可能	サービス仕様（機能仕様）として契約書／利用マニュアルに記載されている場合は必ずしも SLA で定義される必要はない

別表

種別	サービスレベル項目例	規定内容	測定単位	設定例	備考
	外部接続性	既存システムや他の SaaS 等の外部のシステムとの接続仕様（API、開発言語等）	有無	API（プログラム機能を外部から利用するための手続き）を公開	API がインターネットの標準技術で構成され、仕様が公開されており、API の利用期限や将来の変更可能性が明記されていることが望ましい
	同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	有無（制約条件）	50 ユーザ（保証型）	同時接続の条件（保証型かベストエフォート（最善努力）型か)、最大接続時の性能について明示されていることが望ましい

◆サポート

サービスレベル項目例	規定内容	測定単位	設定例	備考
サービス提供時間帯（障害対応）	障害対応時の問合せ受付業務を実施する時間帯	時間帯	24 時間 365 日（電話）	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる
サービス提供時間帯（一般問合せ）	一般問合せ時の問合せ受付業務を実施する時間帯	時間帯	営業時間内（電話） （年末年始・土日・祝祭日を除く） 24 時間 365 日（メール）	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる

別表

◆データ管理

サービスレベル項目例	規定内容	測定単位	設定例	備考
バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有無／内容	有 （日次でフルバックアップ。遠隔地のデータセンタにテープ形式保管。アクセス権はシステム管理者のみに制限。復旧／利用者への公開の方法は別途規定）	保証要件を設定している場合は、具体的に明示。バックアップ内容は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる。 また、SaaS ベンダの民事再生、破産等によりサービス継続が出来ない場合についても明示されていることが望ましい。
バックアップデータの保存期間	データをバックアップした媒体を保管する期限	時間	5 年以上（基幹業務） 3 ヶ月以上（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討
データ消去の要件	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	有無	サービス解約後 1 ヶ月以内にデータおよび保管媒体を破棄。	解約時には、CSV などの一般的なフォーマットでデータ出力ができることが望ましい。

◆セキュリティ

サービスレベル項目例	規定内容	測定単位	設定例	備考
公的認証取得の要件	JIPDEC や JQA 等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）が取得されていること。	有無	ISMS 認証取得 プライバシーマーク取得	IT サービスマネジメントのベストプラクティスである ITIL や JIS Q20000 等の取得状況も確認することが望ましい。
アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること。	有無／実施状況	有 （年１回、外部機関によりサービスの脆弱性に関する評価を受け、速やかに指摘事項に対して対策を講じる。）	セキュリティ監査、システム監査、ペネトレーションテスト等ネットワークからの攻撃に対する検証試験、ウェブアプリケーションの脆弱性検査、データベースセキュリティ監査などを想定。

別表

サービスレベル項目例	規定内容	測定単位	設定例	備考
情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること。	有無／設定状況	有 （利用者のデータにアクセスできる社員等はセキュリティ管理者の許可を得た者に限る。）	
情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること。	有無／	有 （オフィスは IC カードによる運用で執務室に入室可能な社員等を最小限に制限しており、PC はすべてシンクライアントである）	
通信の暗号化レベル	システムとやりとりされる通信の暗号化強度。	有無	SSL、あるいは VPN	SSL の場合は、SSL3.0/TLS1.0（暗号強度 128 ビット）以上に限定。