資料4－4

ＡＳＰ・ＳａａＳの情報セキュリティ対策に関する研究会

報告書

～「ＡＳＰ・ＳａａＳにおける情報セキュリティ対策ガイドライン」の策定～

（案）

ＡＳＰ・ＳａａＳの情報セキュリティ対策に関する研究会

平成２０年　月

目　　次

序　章　はじめに

【１】 ブロードバンド環境の進展

我が国のインターネット人口普及率は平成１８年に 68%[1]を超え、実に国民の３人に２人がインターネットを利用するに至っている。また、平成 18 年度末時点のブロードバンド契約数は 2,644 万契約[2]に達しており、我が国のブロードバンド環境は急速な広がりを見せていることが分かる。ブロードバンドの普及により、音楽・映画等の大容量コンテンツの流通が可能になる等、インターネットの利用形態はますます多様化・高度化し続けており、インターネットは、国民生活・社会経済活動を支える重要なインフラとして、なくてはならないものとなっている。

【２】 国際競争力・生産性向上への取組の強化

我が国は、人口減少社会が現実のものとなり、従来の経済成長モデルは限界を迎えつつある。このような状況において、我が国経済を新たな成長のトレンドに乗せるためには、ICT による生産性向上・国際競争力の強化が不可欠である。このような現状において、経済財政諮問会議が平成 19 年 4 月に取りまとめた「成長力加速プログラム」においては、生産性の相対的に低い分野の効率性アップを図る「サービス革新戦略」の１つとして、「IT の本格的活用を通じて、ネットワーク化や組織革新等を進め、新成長基盤の効率化を図る。」とする「IT 革新」による生産性向上が不可欠であるとしている。その中で、「IT 革新」のための具体的な取組として「ASP（Application Service Provider）や SaaS（Software as a Service）など中小企業にとって使いやすい新たなサービスの普及促進のための共通基盤の整備等環境整備を推進する。」としており、「ASP・SaaS」の重要性が指摘されている。また、「ICT 国際競争力懇談会 最終取りまとめ」(平成 19 年４月　総務省)では、経済成長、生産性向上の基本戦略として、「ASP・SaaS の普及促進」が掲げられている他、「経済財政の基本方針 2007」(平成 19 年６月　閣議決定)「重点計画-2007」(平成 19 年７月 IT 戦略本部)等においても、「ASP・SaaS」の重要性に言及されており、現在、国際競争力強化・生産性向上への切り札として、まさに政府一体となって ASP・SaaS の普及促進に取り組んでいるところである。

【３】 研究会開催の目的

企業等における生産性向上に向けた取組としては、組織間におけるシステム連携の推進や労働力の質の向上等、様々な手段が考えられるが、ASP・SaaS の利用は、自前で開発するよりも短期間でシステムの構築・運用が可能となるほか、当該システムの保守・運用・管理にかかる負担が軽減される等、コストや ICT リテラシー対応等の面で大きなメリットがある。そのため、特に大企業に比べて人的・金銭的資源に限りのある中小企業において

---

1 出典：総務省「通信利用動向調査(世帯編)」(平成１８年度調査)

2 出典：総務省「平成１９年版 情報通信白書」

は、ASP・SaaS の利用が生産性向上に威力を発揮することとなる。

しかし、その一方で、ASP・SaaS 事業者及びその関係組織に利用者である企業等の膨大な機密情報・顧客情報等の情報資産が集積されることとなるため、ASP・SaaS サービスが健全に発展していくためには、ASP・SaaS 事業者における適切な情報セキュリティ対策の実施が重要である。しかし、現状では、「多数を占める中小の ASP・SaaS 事業者においても適切な情報セキュリティ対策が施されているのか」、或いは、「講じるべき情報セキュリティ対策の基準が不明瞭ではないか」、また、「利用者に対して必ずしも十分な説明や情報開示が成されていないのではないか」といった問題点が指摘されているところである。

本研究会では、適切な情報セキュリティ対策が施された ASP・SaaS サービスの提供が促進され、ASP・SaaS が企業等の生産性向上の健全な基盤となるよう、ASP・SaaS サービスの実態、情報セキュリティ対策の現状、今後の進展等を把握した上で、ASP・SaaS 事業者が講ずべき情報セキュリティ対策を、提供するサービス種別の特性に沿って検討した。

第１章　ASP・SaaS サービスに関する諸動向

１．１　ASP・SaaS サービスとは

１．１．１　ASP・SaaS サービスの定義

ASP(Application Service Provider)及び SaaS(Software as a Service)は、ともにネットワークを通じてアプリケーション・サービスを提供するものであり、基本的なビジネスモデルに大きな差はないものと考えられる。

従って、本研究会では、ASP インダストリ・コンソーシアム・ジャパン[3]（以下、「ASPIC Japan」と呼ぶこととする。）の発行した 2004 年版「ASP 白書」による ASP の定義「ネットワークを通じて、アプリケーション・ソフトウェア及びそれに付随するサービスを利用させること、あるいはそうしたサービスを提供するビジネスモデルを指す」を採用するとともに、ASP と SaaS を特に区別せず、「ASP・SaaS」と連ねて呼称することとした。また、ASP・SaaS といった形態で提供されるサービスを「ASP・SaaS サービス」と呼び、ASP・SaaS サービスを提供する主体を「ASP・SaaS 事業者」と呼ぶこととした[4]。

１．１．２　ASP・SaaS サービスの形態

(a) 提供方法

ASP・SaaS サービスでは、利用者がアプリケーションソフトを自らのシステムないしパソコン等にインストールすることによってその機能を利用するのではなく、ASP・SaaS 事業者がユーザの必要とするアプリケーション機能をネットワーク経由で提供する形態をとっている。具体的には、利用者は ASP・SaaS 事業者の保有するサーバにインターネット等を経由して接続し、主に Web ブラウザを通じて ASP・SaaS 事業者から提供されるアプリケーション機能を利用する。

(b) 利用方法

パッケージソフトでは 1 つのソフトウェアを複数の利用者で共同利用することはあまり無いが、ASP・SaaS においては複数の利用者によるソフトウェアの共同利用が前提となっている。ここでいう利用者は、ある法人内の利用者だけを意味するのではなく、法人そのものを含んでいる。つまり、ASP・SaaS サービスの利用においては、パッケージソフトではあまり見られない、法人を跨いだソフトウェアの共同利用も可能となる。

---

[3] 平成 11 年に任意団体として誕生。その後、平成 14 年 2 月に特定非営利活動法人(NPO)の認証を取得。ASP を活用した情報サービスにより、社会生活の改善及び企業の活性化の更なる促進を図ることを目的に、市場活性化支援等の活動を推進している。会員数は 134 社(平成 19 年 10 月現在)。

[4] 本研究会では、一 ASP・SaaS 事業者が一 ASP・SaaS サービスを提供する場合を基本としているが、一 ASP・SaaS 事業者において複数の ASP・SaaS サービスを提供する場合、各 ASP・SaaS サービスを提供するそれぞれの担当部署等の主体が ASP・SaaS 事業者としての「主体」であるとみなすこととした。

(c) 課金

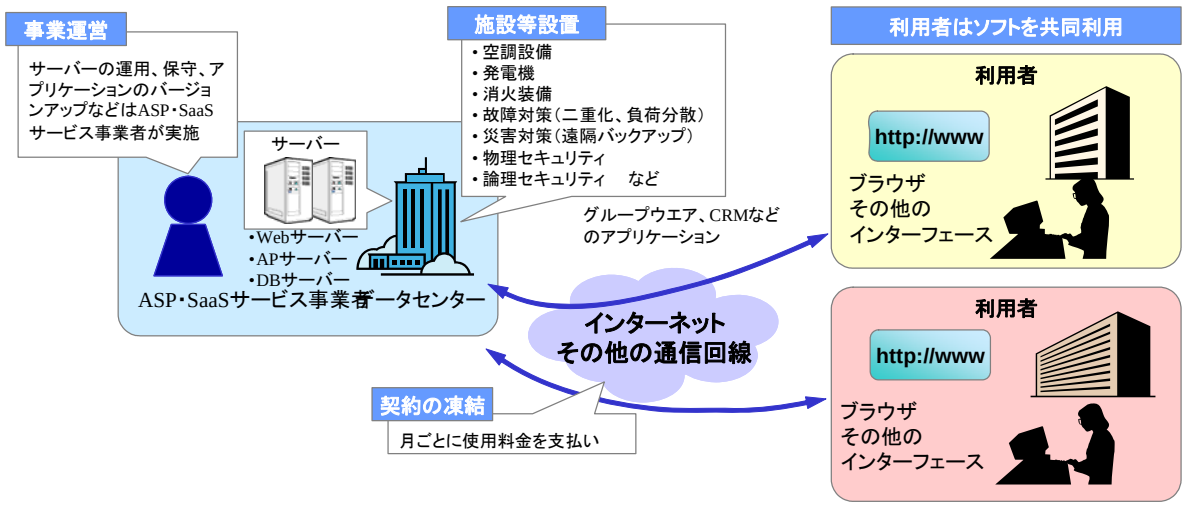
通常のパッケージソフトウエアでは、購入時に一括してライセンス料を支払うことが多い。一方で、ASP・SaaS サービスの場合は、使用時間等に応じて、定期的に使用料金を支払うことが一般的である。

(d) 運用

サーバ等の事業用システムやアプリケーションの運用・保守は、ASP・SaaS 事業者により行われるため、利用者が直接運用・保守をする必要がない。また、事業用システムをデータセンタに設置し、その運用・保守をデータセンタに委託する場合もある。

図表１は、ASP・SaaS サービスの提供・利用形態の全体像を簡潔に整理したものである。

図表 1　ASP・SaaS サービスの提供・利用形態



１．１．３　ASP・SaaS サービスによる利用者のメリット

ASP・SaaS サービスを利用することによって利用者が享受することができるメリットとしては、大きく「コスト面の負担軽減」「迅速且つ柔軟なシステム利用」「ICT リテラシー対応」の３つにまとめることができる。

(a) コスト面の負担軽減

ASP・SaaS サービスは、インターネット環境と Web ブラウザのインストールされたパソコンがあれば利用が可能なため、自前で社内システム等を構築する必要がなく、システム導入に係る巨額な初期投資が不要となる。また、サーバ管理等のシステムの運用に関し

ても、サーバ等を保有する ASP・SaaS 事業者により実施されるため、システム運用に係る人的・技術的コストを大幅に削減することができる。

(b) 迅速且つ柔軟なシステム利用

ASP・SaaS サービスは、利用したいアプリケーションを利用したいときにだけ導入することが可能なため、自前で社内システムを構築・運用しアプリケーションを導入するのに比べ、短期間で迅速な対応が可能となる他、様々な利用シーンに合わせてアプリケーションをカスタマイズする等の柔軟な運用が可能となる。

(c) ICT リテラシー対応

システムの運用・保守には、新たな技術に対応するための高度な ICT 技術の獲得が必要になるが、特に大企業に比べて人的資源に限りのある中小企業にとっては、ノウハウの習得・維持に困難がつきまとう。しかし、ASP・SaaS サービスを活用することによって、専門事業者による高いレベルのノウハウでのシステム運用・保守が可能となる。

また、二次的なメリットとして、情報セキュリティ対策への対応が容易になると考えられている。なぜならば、ウイルス対策ソフトのパターンファイルの更新や、ソフトウェアのパッチの適用等、随時対応が求められる運用は ASP・SaaS 事業者によって実施されるため、更新や適用のし忘れといった運用上のリスクが大幅に低減されると考えられるためである。

１．２　 ASP・SaaS サービスの進化

１．２．１　 ASP・SaaS サービスにおける技術の進歩

ASP・SaaS サービスで用いられる技術は、2005 年を境に大きく進歩したと考えられる。2005 年以前と以後で、ASP・SaaS サービスの主要な技術等の進歩を図表２にまとめた。

図表 ２　2005 年を挟んだ ASP・SaaS サービスにおける技術等の進歩

	1998～2004 年頃		2005 年頃～
ネットワークと端末	インターネット／PC		専用線、その他／ モバイル、電子タグ
対象顧客	BtoB(法人)／BtoG(公共)／ GtoG(公共対公共)		BtoC(対個人)／GtoGtoC
料金	有料		無料
提供するサービス	アプリケーション		認証・決裁等の プラットフォーム機能
利用者	不特定	＋	特定(共同利用)
操作性	応答性が悪く、 操作性は今一つ		Ajax の採用などにより向上
サーバの共有化形態	シングルテナント 一部マルチテナント		マルチテナント バーチャライジング
ソフトウェアコードの 同一化	×(部分的には異なる)		○(記述言語等を統一)
ユーザのカスタマイズの 可否	×(カスタマイズ不可)		○(メタデータの採用等)
他のアプリケーション／ サービスとの連携	×(連携不可)		○(連携用 API を公開等)

出典：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）を基に作成

１．２．２　技術の進歩が ASP・SaaS サービスに与えた影響

ASP・SaaS の進化においては、ブロードバンドの普及により大容量データの送受信が可能になる等、技術の進歩が大きな影響を与えている。特に以下の３つの要素は、アプリケーション連携等、現在のＡＳＰ・SaaS の特徴であり優位性となっている機能を実現するためになくてはならない技術となっている。

(a) Ajax の採用

ASP・SaaS サービスの操作性は 1995 年の Java[5]の発表以来変化を遂げ、2005 年頃より Ajax の採用により飛躍的に向上した。この Ajax[6]ではサーバと非同期に動的にページの一部を書き換えることが可能である。これにより、非常に早いレスポンスを利用者に返すことが可能であるため、操作性は飛躍的に向上した。

(b) マルチテナントによるサーバの共有化

サーバの共有化形態に関しては、以前はシングルテナントが主流であったが、現在はマルチテナント[7]が主流になり、実装にはバーチャライジング[8]が使用されている。これにより、システムの使用状況に応じて動的にリソースをアプリケーションに割り当てる等、ASP・SaaS サービス運営の効率化が進み、コスト的にも有利になった。

(c) ソフトウェアコードの同一化

ソフトウェアコードの同一化については、標準化の進展に伴って記述言語等の統一化が可能となったため、様々なシステム連携が可能となった。その結果、昨今では連携用の API 公開も頻繁に実施されている。この API 公開によって、自らの ASP・SaaS サービスに他の ASP・SaaS サービスを組み込むことにより、異なるアプリケーション同士が統合・連携した新たなサービス形態が、現在では実現されている。

---

[5] Sun Microsystems 社が開発したプログラミング言語及びその実行環境のことで、OS 等のプラットフォームに依存しないという特徴を持つ。

[6] ブラウザ内で動作する JavaScript 言語を用いて、ユーザーインタフェースを実装する技術のことで、ダイナミック HTML と組み合わせることにより、操作性の高いアプリケーションが構築可能である。

[7] ASP・SaaS サービス用の 1 つのサーバ(システム)を複数の利用者で共有するサービス提供形態のことである。

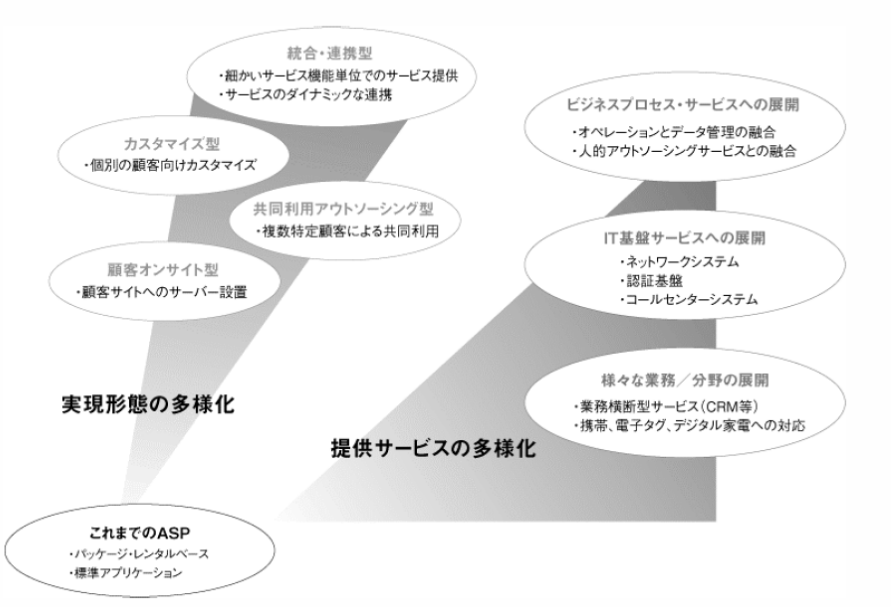
[8] 複数のサーバを 1 つのサーバであるように仮想化する技術のことである。

１．３　 ASP・SaaS サービスの多様化

１．３．１　 ASP・SaaS サービスの多様化

近年、従来と異なる様々な領域で ASP・SaaS サービスの活用事例が拡大している。当初の ASP は、グループウェア等の標準的なアプリケーションを、不特定多数のユーザにレンタル形式で提供するものが主流であった。しかし、図表３に示すように、最近では、実現形態、提供サービスの二つの側面から ASP・SaaS の進化が急速に進展している。

図表 ３　ASP・SaaS の実現形態・提供サービスの多様化



出典：2005 年 ASP 白書 ASPIC Japan／マルチメディア振興センター

(a) 実現形態の多様化

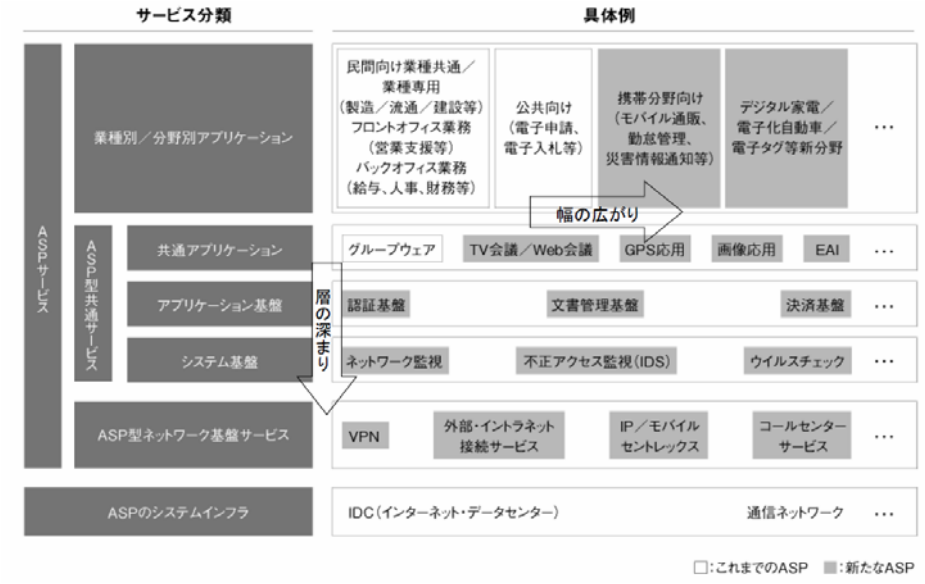
実現形態の面では、前述した異なるアプリケーション同士の「統合・連携型」や、個々の利用者ごとにアプリケーションをカスタマイズして提供する「カスタマイズ型」、地方自治体等に見られる複数の特定顧客による「共同利用アウトソーシング型」、利用者側にサーバ等の機器を設置する「顧客オンサイト型」等、従来に比べその実現形態は様々な広がりを見せている。

(b) 提供サービスの多様化

提供サービスの多様化の面では、図表４に示すとおり、ASP・SaaS 事業者が提供する ASP・SaaS サービスの対象業務・分野の拡大や、パソコンだけではなく携帯電話や電子

タグ等での利用にも対応した利用端末の多様化といった「幅の広がり」に加え、認証基盤や決済機能のようなアプリケーションに共通的なプラットフォームの提供、コールセンタ等の業務アウトソーシングと融合したビジネスプロセス・サービスや VPN・イントラネット接続等のネットワーク基盤の提供といった、ASP・SaaS サービス相互が階層的な関係を持つ「層の深まり」が進んでいる。

図表 4　ASP の提供サービス体系：幅の広がりと層の深まり



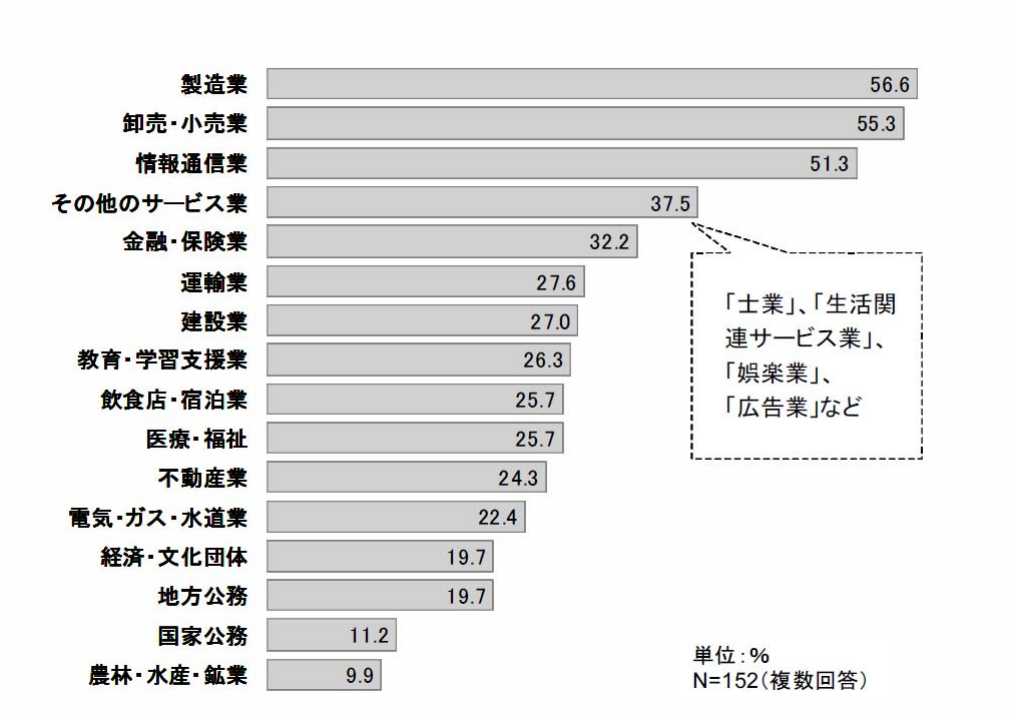
出典：2005 年 ASP 白書 ASPIC Japan／マルチメディア振興センター

１．３．２　利用者の多様化

上記のような ASP・SaaS サービスの進化に呼応して、ASP・SaaS の利用者層も広がりを見せてきた。図表５に示すように、ASP・SaaS サービスの利用者分布はあらゆる業種に広がりを見せており、ASP・SaaS サービスの利用が広範に浸透している状況が伺える。特に「製造業」「卸売・小売業」「情報通信業」の３分野に関しては、２社に１社が何かしらの ASP・SaaS サービスを利用しており、また、「金融・保険業」「医療・福祉」「電気・ガス・水道業」さらには、「地方公務」「国家公務」といった社会インフラに位置付けられる分野においても、ASP・SaaS サービスの利用が進んでいることが分かる。

このような利用者の多様化の背景には、詳細は後述することとするが、営業支援や会計業務といった各分野に共通な ASP・SaaS サービスに加え、業務を横断して利用したり、特定の業務に特化した形の ASP・SaaS サービスの提供が拡大してきたことが大きく影響しているものと考えられる。

図表 ５　ASP・SaaS サービスの利用者業種分布



出典：2005 年 ASP 白書 ASPIC Japan／マルチメディア振興センター

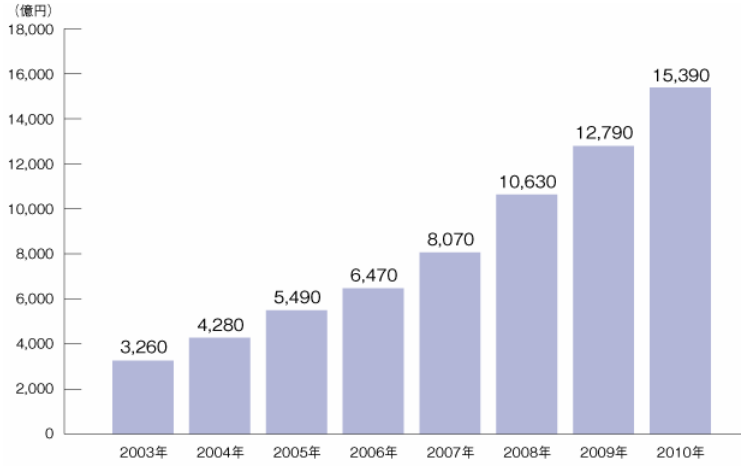
１．４　ASP・SaaS サービスの市場動向

１．４．１　ASP・SaaS サービスの市場規模の推移

ASP・SaaS サービスは、平成１５年以降急速に普及・拡大を続けている。ASP・SaaS サービスの市場規模の推移及び今後の予測を示したものが図表６である。

この調査・予測に基づくと、平成１５年時点で 3,260 億円であった市場規模が、毎年前年比 1.3 倍前後のペースで拡大を続け、平成２２年では平成１５年度に比べ実に５倍弱となる 15,390 億円に達すると予測されている。

図表 ６　日本における ASP・SaaS サービス関連市場の規模の推移と予測



注：ASP関連市場には、セキュリティ・ホスティング等のデータセンターを含む。
情報通信白書2002のASP市場予測、データセンター市場規模予測、eラーニング白書のeラーニング市場のうちシステム事業に分類される事業のベンダー売上げとASP化が見込まれる領域の売上げ、e-Japan関連予算のうち、「行政の情報化及び公共分野における情報通信技術の活用」に対する予算額、ASP関連市場に投下される予算額について、それぞれパラメータを設定して推計した。

出典：2005 年 ASP 白書 ASPIC Japan／マルチメディア振興センター

また、平成９年以降、新たに提供が開始された ASP・SaaS サービスの数をまとめたものが図表７である。

この調査によると、平成９年から平成１１年までの間わずか４件しか新たな ASP・SaaS サービスの提供が開始されていなかったにも関わらず、平成１２年以降は毎年１０件以上、多い年には３６件もの新たな ASP・SaaS サービスの提供が開始されていることが分かる。

図表 7　新たに提供が開始された ASP・SaaS サービス数の推移

サービス提供開始時期	開始サービス数(比率 %)	累積比率(%)
2006 年(1 月～5 月)	11　(7.8)	7.8
2005 年	36　(25.2)	33.0
2004 年	14　(9.8)	42.8
2003 年	27　(18.9)	61.5
2002 年	19　(13.3)	75.0
2001 年	17　(11.9)	86.9
2000 年	15　(10.5)	97.4
1997 年～1999 年	4　(2.8)	100.0

出典：2005 年 ASP 白書 ASPIC Japan／マルチメディア振興センター

１．４．２　ASP・SaaS サービスの普及・拡大の要因

ASP・SaaS サービスが、近年ここまで急速に普及・拡大を続けている背景には、以下の３点の要因が考えられる。

(a) ブローバンドの普及

ASP・SaaS サービスの最も大きな普及要因として、ブロードバンド環境の進展が挙げられる。図表８が示すように、平成１３年時点で 387 万契約だったブロードバンド契約者数は、平成１４年で約 2.5 倍の 943 万契約に急速に拡大、その後も順調に契約者数は増え続け、平成１８年度では 2,644 万契約にまで契約者数を伸ばしている。

ブロードバンドの普及により、音楽・映画等の大容量コンテンツの流通が可能になると共に、データの送受信に係るストレスも大幅に改善されたことが、インターネットを経由し Web ブラウザを通してアプリケーションを利用するという ASP・SaaS サービスの利用を快適なものとし、ASP・SaaS サービスの普及・拡大に拍車をかけたものと推測される。

(b) 個人情報保護法の施行等による企業の意識の変化

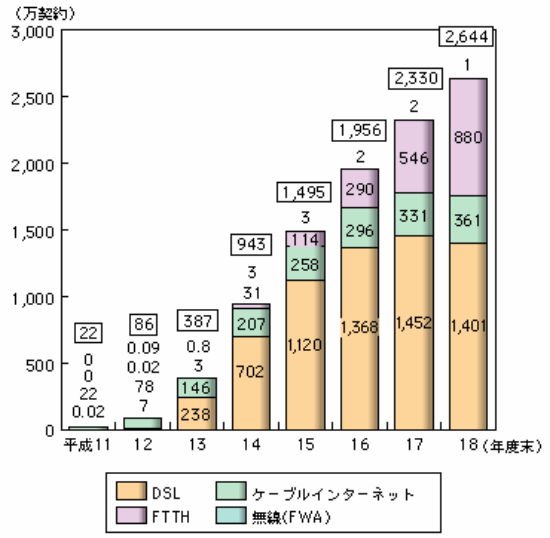
平成１５年の「個人情報の保護に関する法律」の施行されたことに伴い、顧客データ等の適切な管理が企業等に求められるようになった。それに伴い、企業等における情報セキュリティ対策のあり方が見直され、情報システムの運用・管理に係るコストが大幅に増大することとなった。人的・金銭的リソースに限りのある中小企業にとっては、この変化への対応が困難であり、高いレベルのノウハウで運用・管理を任せることのできる ASP・

SaaS サービスの利用が促進されることとなったと考えられる。また、今後施行されることとなる日本版 SOX 法への対応という面でも、ASP・SaaS サービスにかけられている期待は大きい。

⑹ ＡＳＰ・SaaS サービスの多様化

前述したとおり、ASP・SaaS サービスの実現形態や提供サービスは多様化し続けており、より利用者のニーズに合った ASP・SaaS サービスの提供が拡大したことも ASP・SaaS サービスの普及・拡大の一因になっているものと考えられる。

図表 ８　ブロードバンド契約者数の推移



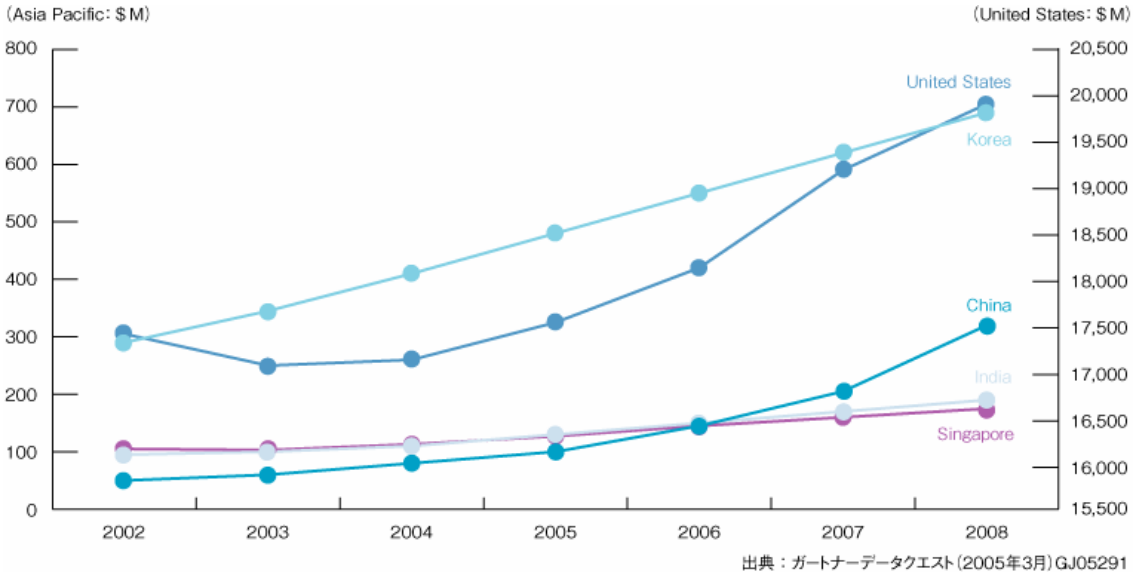
※　平成16年度分以降は電気通信事業報告規則の規定により報告を受けた契約数を、それ以前は事業者から任意に報告を受けた契約数を集計

出典：総務省「平成１９年版 情報通信白書」

１．４．３　　ASP・SaaS サービスの海外における市場動向

海外における ASP・SaaS サービスの市場動向を示したものが図表９である。米国・韓国等、特に ICT 基盤が高度に整備された国においては、ASP・SaaS サービスの市場の伸びが著しいことが分かる。ブロードバンド環境が広く整備された我が国においても、米国・韓国と同様に、今後さらなる ASP・SaaS サービスの市場拡大が期待できる。

図表 9　海外における ASP・SaaS サービスの市場動向



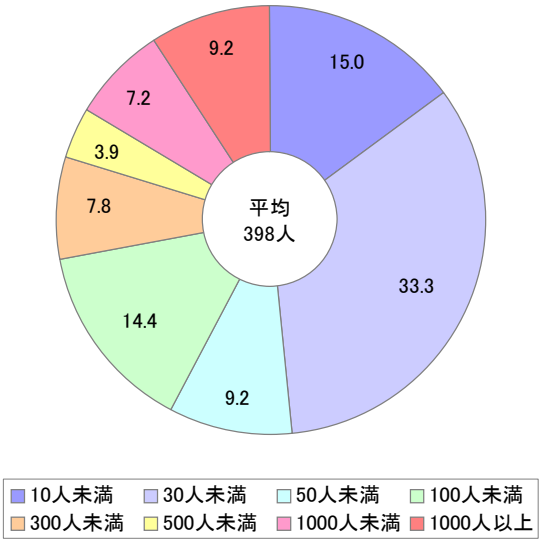
出典：第１回会合資料より抜粋

１．５　ASP・SaaS 事業者及びサービスの現状

１．５．１　ASP・SaaS 事業者の規模

図表 10 より、ASP・SaaS 事業者 1 社あたりの平均従業員数は 398 人、従業員数 100 人未満の事業者が全体の 70%以上を占めており、ASP・SaaS 業界は中小事業者を中心に構成されていることが分かる。

図表 10　ＡＳＰ事業者の従業員規模別割合



ｎ＝１５３

出典：2005 年 ASP 白書 ASPIC Japan／マルチメディア振興センター

１．５．２　ASP・SaaS 事業者のサービス領域

ASP・SaaS サービスが多様化を見せていることは前述のとおりであるが、実際に提供されているサービスの構成比率をまとめたものが図表 11 である。

注目すべきは「上記以外のサービス」に分類されるサービスの多さであり、従来の「各分野で共通して利用できるアプリケーション」を「不特定の利用者」が「閉じた形で利用する」というサービスモデルから、電子カルテや建設支援のような特定の業種に特化した ASP・SaaS サービスや、CRM[9]や ERP[10]といった業務・組織を横断して利用できる ASP・

[9] Customer Relationship Management の略号。きめ細かな対応により顧客の利便性と満足度を向上させ、顧客を囲い込むことにより、売上の増加や収益率の改善を目指す経営手法のこと。
[10] Enterprise Resource Planning の略号。企業の経営資源を統合的に管理・配置し、効率的な経営活動の実現を目指す経営手法のこと。

SaaS サービスの提供が進展していることが伺える。

図表 11　ＡＳＰ事業者の業務領域分類

大分類	詳細分類	回答数	構成比
システム管理	運用管理	19	12.3%
	ネットワーク監視	15	9.7%
	セキュリティ管理	10	6.5%
	IT 資産管理	8	5.2%
バックオフィス	販売・仕入管理	17	11.0%
	会計処理	16	10.3%
	人事管理	14	9.0%
	文書管理	13	8.4%
	給与計算	12	7.7%
	財務管理	8	5.2%
	総務・経理	6	3.9%
	生産管理	2	1.3%
フロントオフィス	営業支援	23	14.8%
	受発注システム	21	13.5%
	EDI	14	9.0%
	販売促進管理	7	4.5%
	流通支援	7	4.5%
	商談システム	3	1.9%
EC サポート	EC サイト構築・管理	30	19.4%
	HP 構築・管理	28	18.1%
	Web 通販	26	16.8%
	B2B サイト運営	18	11.6%
	販売支援	17	11.0%
	インターネット予約	17	11.0%
グループウェア	情報共有支援	40	25.8%
	メール配信	34	21.9%
	会員データベース	19	12.3%
	ファイル転送	12	7.7%
その他	e ラーニング	20	12.9%
	環境管理	2	1.3%
	自動翻訳システム	1	0.6%
上記以外のカテゴリー※		61	39.4%

※上記以外のカテゴリーには、以下のようなものが含まれる　　n = 155 （複数回答）

- CRM や ERP などの、業務横断型サービス
- 決済/物流代行や勤怠/損益管理などの、特定業務に特化したサービス
- 電子カルテや建設支援、カー用品検索などの、特定業種に特化したサービス

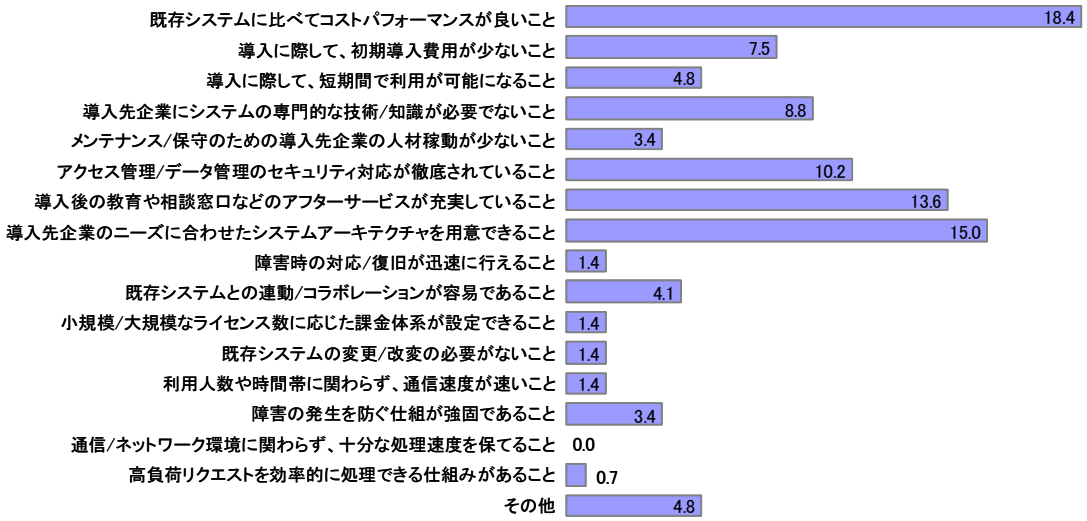
出典：2005 年 ASP 白書 ASPIC Japan／マルチメディア振興センター

１．５．３　ASP・SaaS 事業者が重視している利用者からの期待

利用者から寄せられる ASP・SaaS サービスへの期待の中で、ASP・SaaS 事業者が最も重視している期待をまとめたものが、図表 12 である。

この調査によると、ASP・SaaS 事業者は「コストパフォーマンス」に係る期待を最も重視していることが分かる。この背景には、利用者が ASP・SaaS サービスの選定するにあたり、「コスト」を最も重視しているという現状が伺える。

図表 12　ＡＳＰサービス提供事業者が最も重視している顧客からの期待



ｎ ＝ 147（単一回答）

出典：2005 年 ASP 白書 ASPIC Japan／マルチメディア振興センター

第２章　ASP・SaaS サービスにおける情報セキュリティ対策の現状と課題

２．１　ASP・SaaS 事業者における情報セキュリティ対策の現状と課題

２．１．１　ASP・SaaS 事業者及びサービスの特徴

第１章における ASP・SaaS の動向より、ASP・SaaS 事業者及びサービスの特徴を大きく以下のとおり整理することができる。

・ASP・SaaS 事業者の大半は中小規模の事業者である。
・ASP・SaaS 事業者の提供するサービスは多岐に渡る。

２．１．２　ASP・SaaS 事業者における情報セキュリティ対策に関する仮説

ASP・SaaS 事業者が情報セキュリティ対策を実施する際に直面するであろう課題を検討するにあたり、上記の ASP・SaaS 事業者及びサービスの特徴を踏まえ、以下のような仮説を設定した。

(a) 情報セキュリティ対策の優先付けができていないのではないか

ASP・SaaS 事業者の大半は中小事業者であり、大企業と比較して情報セキュリティ対策に人的・金銭的資源を割くことが困難である。そのため、優先的に実施すべき情報セキュリティ対策を明確にし、重点的に資源配分をすることが求められる。しかし、そのためには、守るべき情報資産の特定や想定される脅威の分析等の一連のリスクアセスメントを実施する必要があり、人的・金銭的資源に限りのある中小の ASP・SaaS 事業者にとっては、大きな困難が伴うことになる。したがって、特に中小の ASP・SaaS 事業者においては、実施すべき情報セキュリティ対策の優先付けがされておらず、不十分もしくは過剰な情報セキュリティ対策がされている可能性がある。

(b) 提供する ASP・SaaS サービスの特徴に基づいた適切な情報セキュリティ対策ができていないのではないか

ASP・SaaS 事業者が提供するサービスは、基幹系業務システムからグループウェアに至るまで実に多岐に渡っており、その取り扱う情報の違いから、各 ASP・SaaS サービスに要求される「機密性」「完全性」「可用性」のレベルも必然的に変わってくる。そのため、一律に情報セキュリティ対策と言っても、「何を」「どの程度」実施すれば良いかはサービスごとに様々であり、自らが提供する ASP・SaaS サービスの特徴を踏まえ、適切に対策を実施する必要がある。しかしながら、上記の仮説のようにリスクアセスメントが適切に実施されていなかった場合、自らの提供する ASP・SaaS サービスの特徴に沿った適切な情報セキュリティができていない可能性がある。

２．１．３　ASP・SaaS 事業者に対するインタビュー調査の実施

上記仮説の検証と課題検討のバックデータに資するため、９社の ASP・SaaS 事業者にインタビュー調査を実施することとした。図表 13 は、インタビューを実施した ASP・SaaS 事業者の一覧である。

図表 13　インタビュー調査を行った ASP・SaaS 事業者の概要

名称	主たるアプリケーション/サービス	売上規模&従業員数	ユーザ企業の状況
A社	財務会計システム	約5,000万円(2006年度)、5名	1,500社、中小企業がほとんど
B社	酒類業販売会計 小売業向け販売会計 店舗管理サポート 請求・指紋認証勤務管理	5.28億円 51名(国内)、100名超(海外含)	中小企業(酒類販売、食品・酒造メーカー)が元々のユーザーである。 現在は、1部上場の大手スーパーマーケット等もユーザである。
C社	各種帳票出力サービス	70億円(2007.2)、203名	金融、メーカー、運輸、教育を中心に大手から中小まで幅広い
D社	企業・自治体・教育機関向けグループウェアサービス	2.4億円、30名	中小・零細企業が多い
E社	社内情報共有サイト、SNS、口コミプロモーション等の作成支援	8.7億円(2007.3)、約150名(連結)、約100名(単体)	200社以上に20,000ID以上を発行(平均で100人/社であり、中小企業が中心と考えられる)。 従業員600名程の企業が最大級のユーザである。
F社	物流・ロジスティクス効率化支援	5.2億円(2006.3)、15名	顧客は大手企業が中心。営業リソースが不足しており、中小企業まで展開できていない。
G社	電車乗り換え案内、地図ASP	20億円、45名	ISP、不動産Webサイト、派遣サイトを中心として、大手から中小まで幅広い
H社	アカウントアグリゲーションサービス インターネットストレージサービス、IDC	99.15億円(2006.3)、420名	大手金融機関、大手コンピュータ企業、化学製品、公共分野
I社	中小企業向けWeb会計システム	3.9億円(2006.3)、23名	業種は問わず、従業員20名以下の中小・零細企業が中心

この度のインタビュー調査では、主に以下の点につき聴取を実施した。

・データセンタ利用の有無
・ユーザ向け接続回線の種別
・システム管理用接続回線の種別
・サーバ/ストレージの運用主体
・他の ASP・SaaS サービスとの連携形態
・情報セキュリティ対策の運用主体
・主な情報セキュリティ対策の内容等
・利用者との情報セキュリティ対策に関する契約への取組及び利用からの要求等

図表 14 及び図表 15 は、インタビュー調査の結果を取りまとめたものである。

図表 14　ASP・SaaS 事業者のインフラとシステム構成

名称	IDC利用の有無	ユーザ向け接続回線の種別	システム管理用接続回線の種別	サーバ/ストレージの運用主体	他社とのASP連携形態
A社	○	インターネットSSL利用	専用回線	自社	自社の会計・給与計算サービスに他社の書式ダウンロードASPサービスを付加して提供している。データ交換はなく、Web表示上の組合せのみ。
B社	X （自社の開発センターに設置）	インターネットSSL利用	インターネットSSL利用	自社	酒販事業者向けの受発注サービスは他社とASP連携（大手他社の卸売業者向けWeb EDIサービス）している。連携他社とサーバー同士で直接データ交換している。
C社	○	インターネットSSL利用	VPN接続	IDCに委託	他社サービス（会計、SCM、CRM等）と積極的にASP連携し、帳票出力サービスを提供。連携他社側が顧客と契約を結び、C社サービスは背後で稼動する。他社サービスとインターネット等を経由してXMLデータ連携している。
D社	○	インターネットSSL利用	VPN接続	自社	提供しているグループウェアサービスにおいて、他社とのASP連携はしていない
E社	○	専用回線	SSHによる専用回線	自社（監視のみIDCに委託）	提供しているサービス（企業向けSNS等）の性格上、ASP連携はしていない。将来他社とのASP連携はしていきたいが、具体的な計画はまだない。
F社	○	インターネットSSL利用	VPN接続	IDCに委託	地図情報について他社のASPサービスと連携（サーバベースで地図情報の提供を直接受けている）。トラック管理サービスとの連携を模索中。
G社	○	帯域保証回線	帯域保証回線	自社	ASP連携はしていない
H社	○	インターネットSSL利用	専用回線	自社	ASP連携はしていない
I社	○	帯域保証専用回線	VPN接続	IDCに委託	SOAPを利用したWebサービスによる連携

図表 15　ASP・SaaS 事業者の情報セキュリティへの取組等

名称	情報セキュリティ対策の運用主体	主たる情報セキュリティ対策の内容等	SLAへの取り組み、利用者からの要求等
A社	自社	•一般的な技術的セキュリティ対策（IPアドレスチェック含む）を自社で構築、運用している •個人情報漏洩保険に加入している（見舞金500円/件）	•SLAに近い記述を利用規約に盛り込んでいる
B社	自社（サーバが設置されている自社開発センターで運用）	•ファイアウォール設置、データのSSL化、不正侵入検知などの一般的な対策のみを講じている	•データの外部委託を嫌う企業が存在する反面、全てをこちらに委ねる「お任せ型」の企業も存在している
C社	IDCに委託	•セキュリティレベルが自社のサービスに見合うIDCを選定 •ディザスタリカバリのためのバックアップセンター設置まではできていない	•標準的なSLA設定を用意して利用者に提示 •標準以上を求める利用者には同様の機能を持つパッケージ版を勧めている
D社	自社	•ファイアウォール等の一般的な情報セキュリティ対策を実施	•利用者認証については、ユーザ利便性とのバランスを考慮し、パスワード認証に留めている •機密性の高いサービスを提供していないため、利用者からセキュリティ強化を求められたことはない
E社	自社	•一般的な技術的セキュリティ対策（IPアドレスチェック含む）を自社で構築、運用している •利用者への情報セキュリティ対策運用に係る提言も行う	•サーバーのセキュリティ対策を顧客に公開している •サービス開始時に顧客のセキュリティチェックシートに記入・提出を求められることが多い
F社	IDCに委託（IDCのマネジメントレンタルサービス）	•関連会社にデジタルフォレンジックの専門会社があり、フォレンジック対策を特に重視している。対策の意味だけでなく、抑止力としても働くと考えている。	•利用者（個人情報を扱う企業が多い）からIPアドレス/MACアドレスでのフィルタリングを求められることもあり、個別に対応している •契約書では、障害や瑕疵に対する一般的な免責事項を設けている。SLAの追加要求等には応じていない。
G社	自社	•半年毎に脆弱性診断を自ら実施して対策を適用	•検索条件により応答時間が異なるためSLAは未設定
H社	自社	•一般的な技術的セキュリティ対策を全社的に実施	•アカウントアグリゲーションサービスに関しては、委員会が設置され、第3者の外部監査を定期的に受け、その結果を顧客に開示している。
I社	自社	•情報セキュリティ社内基準を設けて、これに基づき、自社により運用	•ユーザに対する最低保証サービスレベルを規定。 •これに基づきIDC運用と社内体制を決めている。

２．１．４　仮説の検証

インタビュー調査の結果を受け、仮説の検証を実施した。

⑷ 情報セキュリティ対策の優先付けができていないのではないか

ファイアウォールを設置する等、一般的な技術的情報セキュリティ対策は全ての ASP・SaaS 事業者で実施されているが、その一方で、情報セキュリティマネジメントを運用・改善していくためのプロセスの策定等の組織・運用に係る情報セキュリティ対策はほとんどされていない。適切なリスクアセスメントの実施のためには、そのための組織体制を整備する必要があり、必要な対策の優先付けをするための体制が整っていないものと認められる。

また、インタビュー調査を実施した ASP・SaaS 事業者の規模は様々であるにも関わらず、実施されている情報セキュリティ対策に大きな違いがなく、リスクアセスメントを通じた対策の優先付けができていないことが伺える。

⑸ 提供する ASP・SaaS サービスの特徴に基づいた適切な情報セキュリティ対策ができていないのではないか

インタビュー調査を実施した ASP・SaaS 事業者の提供するサービスはそれぞれ大きく異なるにも関わらず、ユーザ向け接続回線や主な情報セキュリティ対策の内容等を見る限り、実施している情報セキュリティ対策に大きな差は見られない。また、多くの ASP・SaaS 事業者が、実施している情報セキュリティ対策を「一般的な」と表現していることからも分かるように、現在実施している情報セキュリティ対策は、リスクアセスメントを実施し自らの提供する ASP・SaaS サービスの特徴を反映した、適切な情報セキュリティ対策ではないものと考えられる。したがって、提供する ASP・SaaS サービスの特徴に基づいた適切な情報セキュリティ対策はできていないものと認められる。

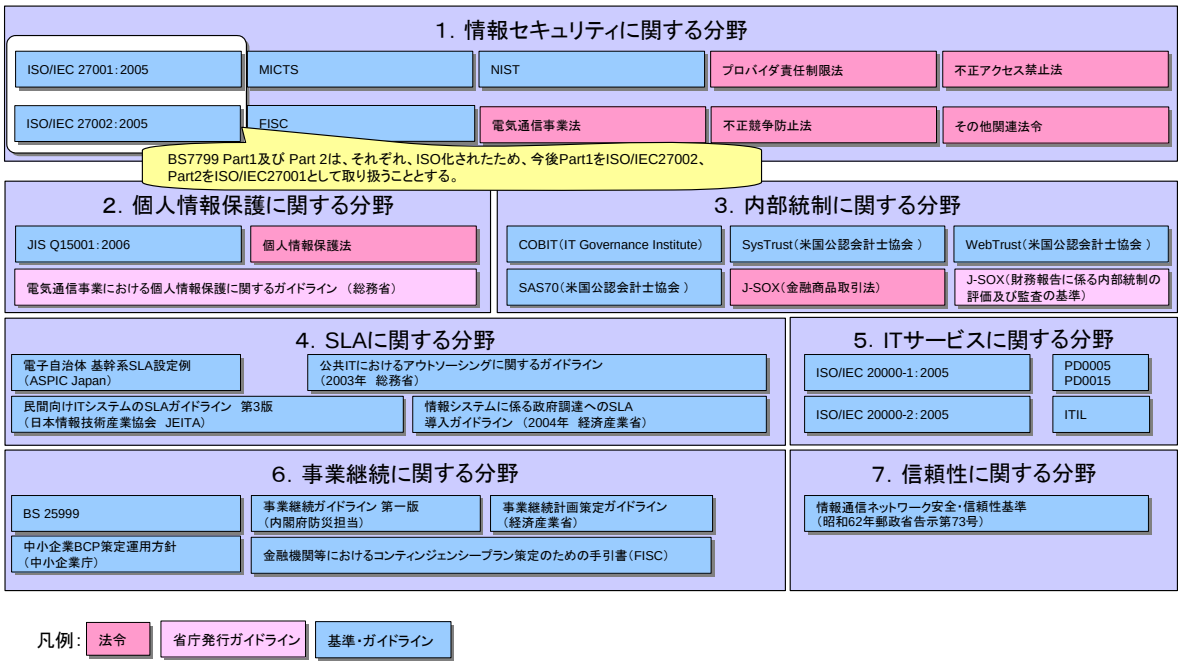
２．２　　現状と課題を踏まえた解決策

２．２．１　　情報セキュリティ対策に関する既存の基準・規範

図表 16 に示すとおり、現在、JIS Q 27001（ISO/IEC 27001）、JIS Q 27002（ISO/IEC 27002）をはじめ、情報セキュリティ対策を実施するにあたっての指針となる基準・規範が多数存在する。しかし、これら既存の基準・指針は、ASP・SaaS サービスの特性を念頭に置いて作成されたものではないため、ASP・SaaS 事業者がこれらの基準・規範をそのまま利活用する場合、ASP・SaaS 事業者の実態に即した情報セキュリティマネジメントが導入・運用しにくいといった問題がある。

ASP・SaaS サービスの特性を反映したガイドラインとして、唯一、総務省の発行した「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」が存在するが、このガイドラインは、地方公共団体が ASP・SaaS サービスを導入する際に、ASP・SaaS 事業者に求めるべき情報セキュリティ要求事項をまとめた利用者目線のガイドラインであり、必ずしもサービスの提供者である ASP･SaaS 事業者にとって利用しやすいものではない。また、公共向け ASP・SaaS サービスのみを念頭に置いて作成されているため、その他 ASP・SaaS サービス一般の特性が反映されているわけではない。

図表 16　情報セキュリティに関係のある既存の法令・基準・ガイドライン等



２．２．２　新たなガイドラインの策定へ

以上の議論の結果、本研究会では、ASP・SaaS サービスの特性を反映し、ASP・SaaS 事業者の実態に即した、新たな情報セキュリティガイドラインを作成する必要があるとの結論に達した。

第３章　情報セキュリティ対策ガイドラインの策定

３．１　ガイドラインに関する基本的な考え方

３．１．１　ASP・SaaS 事業者が情報セキュリティ対策ガイドラインに求める期待

ASP・SaaS 事業者の実態に即した新たな情報セキュリティ対策ガイドラインの策定を検討するにあたり、ASP・SaaS 事業者がガイドラインにどのようなことを求めているかについてインタビュー時に併せて聴取した結果、大きく３点に期待が集まることとなった。実際に寄せられた回答と共に以下に記載する。

(a) 利用者が ASP・SaaS サービスを適切に選別できるような判断基準としての役割

利用者に対して、ASP・SaaS 事業者がどのような情報セキュリティ対策を講じているかが分かるような、また、ISMS 等の認証を取得していなくても、適切な情報セキュリティ対策を実施していることを利用者に伝えられるようなガイドラインへの期待が寄せられた。その一方で、一律にグレード分けをすることにより、人的・金銭的リソース及び運用に係るノウハウの蓄積に乏しい新興 ASP・SaaS 事業者が淘汰されることに対する強い危惧も寄せられた。また、サービス内容やコスト等を勘案した上での「利用者の判断基準」としての役割が求められた。

- ISMS 認証が未取得であっても、本ガイドラインを遵守していることが顧客への PR となれば良い。
- ISMS、P マークと本ガイドラインを組み合わせ、ASP・SaaS 事業者の情報セキュリティ管理制度を説明できることがベストである。
- グレードの上下がすべてを決めるのではなく、サービスグレードとコストのバランスが分かればよい。
- ASP・SaaS 事業者のグレード付けは困難と考えられる。
- 利用者に対して「○○の対策を講じていないため良くない事業者である」ということが見えるような仕組みは、事業者にとってもありがたい。
- 利用者が安心して ASP サービスを利用できるガイドラインを作成してほしい。
- 情報セキュリティに関する認定制度にすると、起業したての面白いベンチャー企業が淘汰される恐れがある。ASP・SaaS 事業者をランク付けする認定制度には賛成できない。

(b) 様々な規模の ASP・SaaS 事業者への対応

ASP・SaaS 事業者の大半を中小が占めるという実態を反映し、ガイドラインに基づく情報セキュリティ対策が、中小 ASP・SaaS 事業者にとって過度な負担を与えるものとなることへの危惧が寄せられた。

- ASP・SaaS 事業者のサービス構築規模に応じたガイドラインが良い。

・ マンパワーを含め、管理コストがかかるガイドラインは望ましくない。
・ 厳格でなく、ベンチャー企業でも対応できるようなレベルを希望している。

⑹ 新規に参入する ASP・SaaS 事業者にとっての指南書としての役割

自らが ASP・SaaS サービスに新規参入した際の経験を踏まえ、初めて ASP・SaaS サービスを開始する事業者にとって、事業立ち上げの際に優先的に実施すべき対策項目や、ASP・SaaS サービスを提供する際に必要となる外部組織の選定基準等も盛り込まれることが期待された。

・ 新たに参入する事業者向けに IDC の選択基準もあると良い。
・ ASP 事業を立ち上げた当時は、ノウハウが分からず苦労した経験があるので、ASP・SaaS サービスの新規参入事業者に対して事業の立ち上げ時にすべきことを指南したガイドラインがあると良い。

ガイドラインの策定にあたっては、これらの期待についても考慮しながら、基本的な考え方を整理した。

３．１．２　ガイドラインに関する基本的考え方とアプローチ

ASP・SaaS における情報セキュリティ対策上の課題解決を図るため、まず、ガイドラインの基本的位置づけを以下のように設定した。

【ガイドラインの基本的位置づけ】

ASP・SaaS 事業者が、提供するサービスの特徴に基づいた適切な情報セキュリティ対策の実施を検討する際の具体的な指針

また、ガイドライン策定にあたっては、以下の重点ポイントを特に考慮することとした（図表 17）。

【ガイドライン策定にあたっての重点ポイント】

- ASP・SaaS 事業者及びサービスの特性を反映し、優先的に取り組むべき情報セキュリティ対策を絞り込むこと

- ASP・SaaS 事業者がガイドラインをそのまま利用することで、比較的簡単に自ら提供するサービスに即した情報セキュリティ対策を実施できるようにすること

- ASP・SaaS 事業者が理解および実施しやすい、具体的な情報セキュリティ対策を

示すこと

なお、基本的位置づけに示したとおり、ガイドラインは ASP・SaaS 事業者が参照して利活用することを念頭において検討を行うが、ASP・SaaS サービスの利用者にとっても理解しやすいものとすることも考慮する。

これらの重点ポイントを満足することで、次のよう効果が見込まれる。

【新たなガイドライン策定により見込まれる効果】

- 情報セキュリティ対策に人的･金銭的な資源を割くことが困難な中小のASP･SaaS事業者や新規参入事業者に対して、個々に対策導出を行う負担を軽減し、優先的に取り組むべき対策の指針を与える

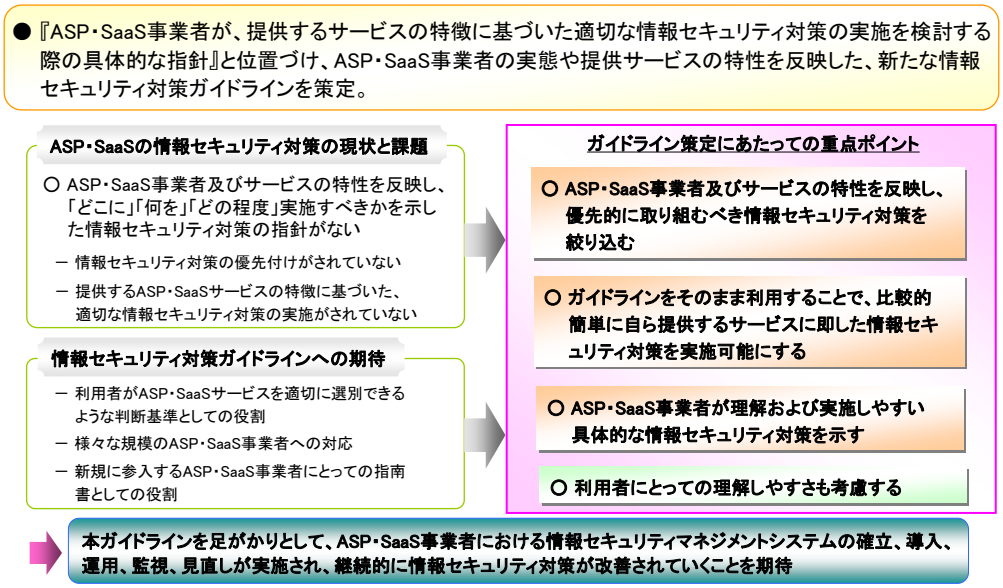
- 他の ASP・SaaS サービスと連携する際、連携 ASP・SaaS 事業者に対する情報セキュリティ対策の要求事項として、本ガイドラインが一定の指針となり得る

- 利用者に対する情報セキュリティ対策状況の提示内容についての一定の指針となり得る

- ASP・SaaS 事業者が実施している情報セキュリティ対策の妥当性を利用者が評価する際の一定の指針となり得る

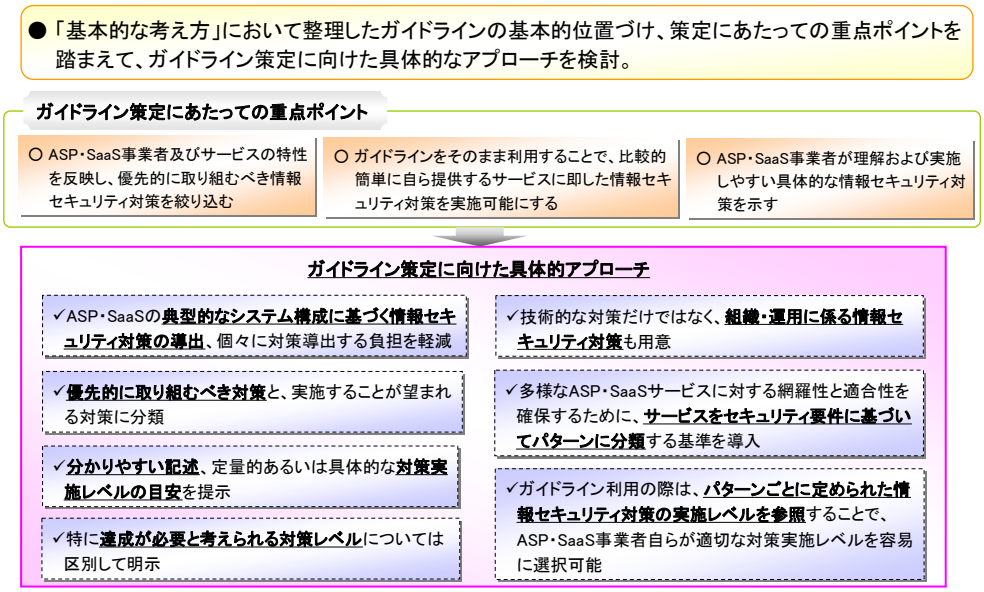
これらの各効果によって、ASP・SaaS 業界全体における情報セキュリティレベルの底上げ、利用者も含めた情報セキュリティに関する意識向上を期待することができる。

図表 17　ガイドラインに関する基本的考え方



さらに、上記の重点ポイントを実現するために、ガイドラインの策定にあたって以下のアプローチを採用することとした（図表 18）。

図表 18　ガイドライン策定へのアプローチ



【ガイドライン策定へのアプローチ】

- ASP・SaaS サービスの典型的なシステム構成に基づいて情報セキュリティ対策を導くことにより、ASP・SaaS サービスに対して重視すべき情報セキュリティ対策項目を絞り込む。ガイドラインで取り纏められている対策項目を実施することにより、ASP・SaaS 事業者が個々に対策導出を実施する負担を軽減する

- 技術的なシステムに特化した個別対策の実施だけではなく、ASP・SaaS 事業者に特化した組織・運用に係る情報セキュリティ対策も用意する

- ASP・SaaS 事業者にとって理解しやすいように、情報セキュリティ対策の内容を事例などを用いて可能な限り分かりやすく記述するとともに、定量的あるいは具体的な対策実施レベルの目安を提示する

- ASP・SaaS サービスにおける適切な情報セキュリティレベルを確保することを促すために、特に達成が必要と考えられる対策レベルについては区別して明示する

- 優先的に取り組むべき対策と、実施することが望まれる対策に分類し、初期導入を

しやすくすると同時に、より高い情報セキュリティレベル実現への道程を示す

- 多様な ASP・SaaS サービスに対する網羅性を実現しつつ個々の ASP・SaaS サービスに適切な情報セキュリティ対策を得るために、ASP・SaaS サービスを、求められる情報セキュリティレベルでいくつかのパターンに分類する基準を導入する

- パターンごとに適切な情報セキュリティ対策の実施レベルを定めておく。ガイドラインの利用の際には、個々の ASP・SaaS サービスがどのパターンに属するかを分類基準により判断し、そのパターンに対応する対策実施レベルを参照するのみで、ASP・SaaS 事業者自らが適切な情報セキュリティ対策の実施レベルを容易に選択できるようにする

また、ガイドラインは JIS Q 27001（ISO/IEC 27001）に示される情報セキュリティマネジメントシステムの考え方を参考として策定し、ガイドラインを足がかりとして、ASP・SaaS 事業者における情報セキュリティマネジメントシステムの確立、導入、運用、監視、見直しが実施され、継続的に情報セキュリティ対策が改善されていくことを期待する。

３．２　　ガイドライン策定に向けた検討

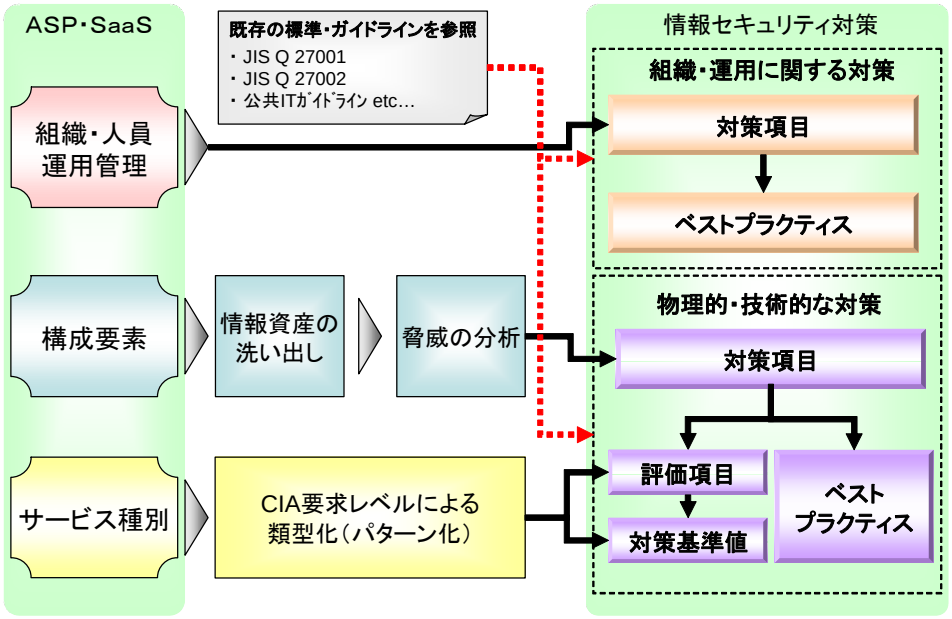
３．２．１　　検討の進め方

本項では、３．１項に記載したガイドラインに関する基本的な考え方等を踏まえ、ガイドライン策定にあたっての全体的な検討の進め方について述べる。

ASP・SaaS における情報セキュリティ対策としては、情報セキュリティ対策の継続的な改善を図るため、ASP・SaaS 事業者内組織における運用管理体制の整備、外部組織との契約における留意事項等の組織・運用面での対策、並びに ASP・SaaS サービスの情報資産を保護するため、システムを構成するハードウェア、ソフトウェア及び建物・電源等のハウジング等に施す物理的・技術的な対策が必要となる。

以上を踏まえて、ASP・SaaS サービス情報セキュリティ対策導出の流れを図表 19 に示す。以下、各手順について説明する。

図表 19　ガイドライン策定に向けた検討の流れ



【１】 組織・運用に関する情報セキュリティ対策の導出

① 情報セキュリティマネジメントにおけるステークホルダの確認

情報資産を確実に保護し、さらに継続的な改善を図るためには、単に物理的・技術的な対策を施すのみではなく、組織・運用に係る情報セキュリティ対策が必要である。このため、まず、ASP・SaaS サービスの提供業務の中で、重点を置いて考慮すべきステ

ークホルダの確認を行う。

② 対策項目の導出

網羅性の非常に高い JIS Q 27001 附属書 A の情報セキュリティ詳細管理策を参考として、ASP・SaaS サービスのステークホルダ構成に即した対策項目を導出する。ここで導出する対策項目は、情報セキュリティへの取組の基本方針及び組織管理についての基本事項に加えて、以下に係る詳しい内容を含んでいる。

- 連携 ASP・SaaS サービス事業者との取り決め
- 情報資産管理
- 従業員管理
- 情報セキュリティインシデント管理
- コンプライアンス
- サービスサポート責任

③ ベストプラクティスの作成

対策を実施するにあたっての具体的な実施方法や注意すべき点をまとめた事例集である「ベストプラクティス」を対策項目ごとに作成する。ガイドラインには、ASP・SaaS に特化された対策項目に加え、ベストプラクティスを併記することで、対策実施内容の理解促進を図る。

【2】 物理的・技術的な情報セキュリティ対策の導出

① ASP・SaaS サービスの類型化(パターン化)

多様な ASP・SaaS サービスに対する網羅性を確保しつつ、個々の ASP・SaaS サービスに適切な情報セキュリティ対策を得るために、ASP・SaaS サービスの類型化(パターン化)による分類を検討する。

具体的には、ASP・SaaS サービスに対して要求される情報セキュリティレベル(「機密性(C:Confidentiality)」「完全性(I:Integrity)」「可用性(A:Availability)」、以下、”CIA”という。)の各々の要求レベルに基づいたパターン分類の基準を検討する。また、ASP・SaaS として提供されている代表的なサービス種別群を用いながら、適切なパターン分類が可能となるよう、パターン分類基準の詳細検討を行う。

② 構成要素の特定

ASP・SaaS サービスに特化した情報セキュリティ対策項目を効率的に絞り込むために、まず ASP・SaaS サービスの提供で想定される様々なシステム構成を統合した後、ASP・SaaS サービスの典型的なシステム構成を設定する。次に、典型的なシス

テム構成の中の構成要素(ASP・SaaS サービスの提供に使用するハードウェア、ソフトウェア、通信機器・回線、建物などの固定資産)を特定する。

③ 構成要素に基づく情報資産の洗い出し

各構成要素における情報資産を洗い出しリストアップする。本ガイドラインでは、情報資産を「ASP・SaaS サービスで使用される有形・無形のもの」と定義する。従って、「構成要素における情報資産」とは、構成要素及び各構成要素を介する情報そのものを指すこととなる。

④ 情報資産に対する脅威分析

各情報資産に対する脅威のリストを作成する。脅威のリストは MICTS の手法を用いて網羅的に洗い出し、各脅威が情報資産に対して CIA のどの観点を脅かすものかを特定する。

⑤ 対策項目の導出

情報資産とそれに対する脅威を特定した後、これらに対応する情報セキュリティ対策を導出する。具体的には、網羅性の非常に高い JIS Q 27001 付属書 A に示されている情報セキュリティ詳細管理策を参考にしながら、ASP・SaaS サービスの現状に即した内容となるように情報セキュリティ対策を検討する。ASP・SaaS に特化した情報セキュリティ対策の検討にあたっては、「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」を参考にした。

次に、上記のようにして得られた情報セキュリティ対策群を整理して、「対策項目」を導出する。また、実施の優先度の観点から、対策を「基本」と「推奨」に分類する。

⑥ ベストプラクティスの作成

対策を実施するにあたっての具体的な実施方法や注意すべき点をまとめた事例集である「ベストプラクティス」を対策項目ごとに作成する。多様な ASP・SaaS サービスによって異なってくるセキュリティ要求をカバーするように、様々な実施レベルを想定した事例の検討を行う。ガイドラインには、ASP・SaaS に特化された対策項目に加え、ベストプラクティスを併記することで、対策実施内容の理解促進を図る。

⑦ パターンに応じた対策実施レベルの設定

物理的・技術的な情報セキュリティ対策について、各パターンに求められる CIA 毎の情報セキュリティレベルと、個々の対策項目によってカバーされる脅威が CIA のどの特性を有するかという観点を突き合わせることで、各パターンに対する情報セキュリティ対策実施のレベルを検討する。具体的には、各対策項目についてその実施レベルを

評価する指標である評価項目を設定し、目安となる対策実施レベルをあらわす指標値を「対策参照値」として設定する。評価項目および対策参照値については、「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」を参考にした。

【3】 参考文書

以上の検討にあたり、以下に挙げる既存の標準・ガイドライン等を参考にした：

- JIS Q 27001:2006 (ISO/IEC 27001:2005)
- JIS Q 27002:2006 (ISO/IEC 17799:2005)
- MICTS（Part1: JIS Q 13335-1、Part2）
- 総務省：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
- 金融情報システムセンター：金融機関等コンピュータシステムの安全対策基準・解説書

３．２．２　組織・運用に関する情報セキュリティ対策の導出

ASP･SaaS サービスの情報資産を確実に保護し、さらに継続的な改善を図るためには、単に物理的・技術的な対策を施すのみではなく、組織・運用に係る情報セキュリティ対策が必要である。本項では、組織・運用に関する情報セキュリティ対策を導出する過程について述べる。

【1】 情報セキュリティマネジメントにおけるステークホルダの確認

まず、ASP・SaaS サービスの提供業務の中で、重点を置いて考慮すべきステークホルダの洗い出しを行う。ASP・SaaS サービスの 1 つの顕著な特徴は、ステークホルダの組織及びその要員が多岐に渡ることである。

現在の ASP・SaaS サービスの提供形態について調査した結果、図表 20 に示すようなステークホルダをリストアップした。

図表 20　ASP・SaaS の情報セキュリティマネジメントにおける重要なステークホルダ

ステークホルダ	組織等	要員
サービス利用企業	サービス利用組織	サービス利用者
		利用者の管理連絡窓口
ASP・SaaS 事業者	経営陣	経営者等
	内部組織	管理責任者、その他の管理者
		それ以外の従業員
	ユーザーサポート組織	オペレータ、サポート技術者
	その他	雇用予定者、雇用変更者、雇用終了者
連携 ASP・SaaS 事業者	－	－
その他の外部組織	－	－

【2】 組織・運用に関する情報セキュリティ対策の必要性

【1】でリストアップした各ステークホルダに対して、どのような組織・運用面の対策[11]が必要となるかを検討した。

まず、外部のステークホルダに対しては、要求事項や契約要件等を明確にした上で、これを確実に遵守させることが必要である。このため、契約や SLA 締結等にかかる対策が必

[11] 責任分界明確化、SLA の合意形成、情報セキュリティ要求とその遵守の監視等、ASP・SaaS サービス提供において特に重要な情報セキュリティ対策が存在している。

要となる。

一方、ASP・SaaS 事業者の内部組織については、例えば、社内における基本方針、規程、マニュアル等の約束事を定めた上で、継続的改善を図るための体制とリソースの確保が求められることになる。

【3】 対策項目の導出

図表 22 で示した各ステークホルダに対する組織・運用面の対策を検討するにあたり、網羅性の非常に高い JIS Q 27001 附属書 A に示される情報セキュリティ詳細管理策を参考として対策項目を導出することとした。この際、ASP・SaaS サービスのステークホルダ構成を考慮し、これに即した対策項目として具体化することを試みた。

また、中小企業が多くの割合を占める ASP・SaaS 事業者の事情を考慮し、分かりやすく、かつ中小企業にとっても優先的に取り組むべき対策に重点を置いた検討を行った。この際、類似した対策項目を集約して分かりやすく書き換えて、対策項目数を削減した

組織・運用面の対策の内容の概略を以下に示す。成果として策定された情報セキュリティ対策ガイドラインにおいては、これらの対策を「組織・運用編」としてまとめている。

(a) 基本方針

ASP・SaaS 事業者が組織全体として情報セキュリティに取組むにあたっての基本方針の作成や経営陣の役割について要求している。

(b) 組織管理についての基本的対策

ASP・SaaS 事業者の内部組織及び外部組織（サービス利用企業を除く外部のステークホルダ）に対して行うべき規程、マニュアル、契約等に関する基本的要求事項を大枠でまとめている。

(c) 連携 ASP・SaaS 事業者についての対策

ASP・SaaS サービスのステークホルダとして特徴的な連携 ASP・SaaS 事業者に対する要求事項をまとめている。

(d) 情報資産の管理についての対策

ASP・SaaS 事業者の内部組織及び外部組織（サービス利用企業を除く外部のステークホルダ）に対して、情報資産の管理に特化して適用すべき要求事項を取りまとめている。

(e) 従業員についての対策

ASP・SaaS 事業者の従業員との契約等に特化して適用すべき要求事項を取りまとめて

いる。

(f) 情報セキュリティインシデント対応についての対策

ASP・SaaS 事業者の従業員の情報セキュリティインシデント対応に特化して適用すべき要求事項を取りまとめている。

(g) コンプライアンスについての対策

ASP・SaaS 事業者の従業員に対して、法令や規則を遵守することを要求している。

(h) サービスサポートの責任

連携 ASP・SaaS 事業者との事業連携の中で、ASP・SaaS 事業者のサービスサポート組織が果たすべき役割について要求している。

【4】 ベストプラクティスの作成

ASP・SaaS 事業者が対策項目に対する理解を深めることができるように、対策を実施するにあたっての具体的な実施方法や注意すべき点の解説等をまとめたベストプラクティスを対策項目毎に作成することとする。ガイドラインでは、対策項目とベストプラクティスを併記する。

ベストプラクティスの作成にあたっては、関連分野の専門家(ASP・SaaS 事業者、情報機器メーカ、ISP 及びデータセンタ事業者等)の知見を積極的に取り入れ、実際の ASP・SaaS サービスの状況に沿った内容及び表現となるよう留意した。また、JIS Q 27002 のベストプラクティスも参考とした。

組織・運用面の対策項目に対するベストプラクティスの記述を、図表 21 に例示する。

図表 21　組織・運用面の対策項目に対するベストプラクティスの例

Ⅱ．３　連携 ASP・SaaS 事業者に関する管理

Ⅱ．３．１　連携 ASP・SaaS 事業者から組みこむ ASP・SaaS サービスの管理

Ⅱ．３．１．１　【基本】

連携 ASP･SaaS 事業者が提供するサービスに関する事業者間の合意に含まれるセキュリティ管理策、サービスの定義、及び提供サービスレベルが、連携 ASP・SaaS 事業者によって実施、運用及び維持されることを確実にすること。

【ベストプラクティス】

i. 連携 ASP・SaaS 事業者から ASP・SaaS サービスの提供を受ける場合には、情報セキュリティの取決めについて連携 ASP・SaaS 事業者が確実に実施するように、契約やサービスレベルアグリーメントで要求することが望ましい。

ii. 連携 ASP・SaaS 事業者が提供するサービスの内容が同意なしに変更されたり、サービスレベルが要求を満たさないことが無いように､契約やサービスレベルアグリーメントで要求することが望ましい。

３．２．３　物理的・技術的な情報セキュリティ対策の導出

本項では、ASP・SaaS サービスの構成要素を特定し、情報資産を洗い出した上で、これらを保護するための物理的・技術的な情報セキュリティ対策を導出する。

【１】 ASP・SaaS サービスの類型化(パターン化)

ASP・SaaS 事業者が提供するサービスは多種多様なものが存在しており、各サービスによって取り扱う情報が異なっているため、各 ASP・SaaS サービスに要求される CIA のレベルも必然的に異なってくる。このことは、求められる情報セキュリティ対策において、サービスの種別ごとにレベル差が生じる可能性があることを示している。

本項では、ASP・SaaS サービスの CIA 要求レベルの違いを情報セキュリティ対策の導出に適切に反映することを目的として、ASP・SaaS サービスの類型化(パターン化)を行った。

①　CIA に対する要求レベルの判定基準

ASP・SaaS サービスが取り扱う情報の内容や求められるサービス品質等に着目し、CIA の要求レベルの高低に関する考え方(判定基準)を以下のとおり整理する。

⑴ 機密性への要求

以下の情報を預かる場合には、その件数に関わりなく、機密性への要求は「高い」ものとする。

①個人情報

利用者及び利用者の顧客に関する、特定の個人(生存者)を識別することができる情報。

②営業秘密情報

秘密として管理されている生産方法、販売方法、その他の事業活動に有用な技術上または営業上の情報であって、公然と知られていないもの。

⑵ 完全性への要求

ASP・SaaS 事業者が利用者のデータを管理するという特性上、そのデータに改ざん・削除・漏えい等のインシデントが発生した場合、顧客の事業継続に多大な影響を与えるものと考えられる。また、ASP・SaaS 事業者が提供する情報においても、その情報に改ざん等のインシデントが発生した場合、その情報に依存している顧客にとって大きな損害が発生することが想定される。従って、ASP・SaaS 事業者においては、そのサービス種別に関わらず、完全性への要求は「高い」ものと考えられる。

⑶ 可用性への要求

①可用性への要求が高いサービス

⑷ 運用時間中は原則として必ず稼動させておくことが求められるサービス

⑸ サービスが停止することで、利用者に多大な経済的損失や人命危害が生じる恐れのあるサービス

②可用性への要求がそれほど高くないサービス

⑷ サービスが停止することで、利用者に部分的な経済的損失が生じる恐れのあるサービス

⑸ サービスが停止することで、利用者の基幹業務に明確な影響を及ぼすサービス

③可用性への要求が低いサービス

①及び②に該当しないサービス

② ASP・SaaS サービスのパターン

前項の判定基準に基づくと、完全性への要求は一定であることから、機密性への要求レベル(２段階)及び可用性への要求レベル(３段階)の違いにより、各 ASP・SaaS サービスは以下の６つのパターンに類型化されることになる。

【パターン１】機密性・完全性・可用性の全てへの要求が高いサービス

【パターン２】機密性・完全性への要求は高いが、可用性への要求はそれほど高くないサービス

【パターン３】機密性・完全性への要求は高いが、可用性への要求は低いサービス

【パターン４】機密性への要求は低いが、完全性・可用性への要求が高いサービス

【パターン５】機密性への要求は低いが、完全性への要求は高く、可用性への要求はそれほど高くないサービス

【パターン６】完全性への要求は高いが、機密性・可用性への要求は低いサービス

図表 22 ASP・SaaS サービスのパターン(６種類)

パターン	機密性への要求	完全性への要求	可用性への要求
1	高い	高い	高い
2	高い	高い	中程度
3	高い	高い	低い
4	低い	高い	高い
5	低い	高い	中程度
6	低い	高い	低い

③ ASP・SaaS サービスの類型化結果

前２項を踏まえ、実際に各 ASP・SaaS サービスの CIA に対する要求レベルを判定した。その結果を図表 23 に示す。

図表 23　各 ASP・SaaS サービスの CIA 要求レベル判定結果

大分類	小分類	サービス種別	サービスの定義	機密性			可用性			
				高	低	理由	高	中	低	理由
業務・業種別アプリケーション	フロントオフィス業務	受発注	見積、受発注、請求、支払等を行う EDI 等のサービス	○		営業秘密情報の保持		○		機会損失を生じないことが重要
		購買支援	MRO 電子購買、購買情報公開等の購買支援を行うサービス	○		営業秘密情報の保持			○	
		CRM(顧客管理)・営業支援	顧客管理、営業プロセス支援等を行うサービス	○		一般個人情報等の保持			○	
		販売支援	マーケティングを支援するサービス	○		営業秘密情報の保持			○	
		販売管理・売掛金管理	－	○		営業秘密情報の保持		○		長時間・頻繁の停止は不可
		契約	電子契約を行うサービス	○		営業秘密情報の保持			○	
		広告	クリック型広告等のインターネット広告を行うサービス		○				○	
		公共窓口業務	自治体等の窓口サービス業務を支援するサービス	○		一般個人情報の利用		○		窓口業務は長時間停止が許容されない
	バックオフィス業務	人事給与・勤怠管理・経理	人事(採用管理を除く)・経理の業務を支援するサービス	○		顧客の内部個人情報保持	○			常に稼動の必要あり
		採用管理	人事における採用管理を支援するサービス	○		一般個人情報等の保持			○	
		資産管理	企業の資産管理を支援するサービス	○		営業秘密情報の保持			○	
		ERP(財務会計等)	ERP のうち、財務会計に係るサービス	○		営業秘密情報の保持	○			長時間・頻繁の停止は不可
		IT 資産管理	企業の IT 資産管理を行うサービス		○				○	
		在庫管理	－	○		一般個人情報等の保持		○		長時間・頻繁の停止は不可
	ミドルオフィス業務	e ラーニング・LMS	オンライン教育・試験を提供、支援、計画するサービス		○				○	
			上記のサービスと連携して個人情報を管理するサービス	○		一般個人情報の保持			○	
		ニュースリリース業務	メディアや Web へのニュースリリースを支援するサービス		○				○	
		文書管理	重要文書を含めて管理するサービス	○		営業機密情報の保持	○			常に稼動の必要あり
			重要文書以外を管理するサービス		○			○		長時間・頻繁の停止は不可
	EC サポート業務	EC サポート	電子商取引をアウトソーシングするサービス	○		営業秘密情報の保持	○			常に稼動の必要あり
			電子商取引と物流・決済を一括提供する産地直送等のサービス		○			○		長時間・頻繁の停止は不可
		ネットショッピング支援	仮想店舗貸しサービス	○		一般個人情報等の保持	○			常に稼動の必要あり
			自ら売買することを支援するサービス	○		一般個人情報等の保持			○	
		コールセンター支援	コールセンター業務支援サービス(コールセンターシステムのみのアウトソーシング、受け答え代行も含めたアウトソーシング)	○		一般個人情報等の保持	○			顧客フロントであり、止められない
	業種特化型 ASP	建設業	建設業向け EDI、工事発注、工事総合管理等	○		営業秘密情報の保持		○		機会損失を生じないことが重要
		運輸業	配車計画サービス、ITS 動態管理サービス等		○				○	
		卸売・小売・飲食業	店舗管理、POS 関連サービス(受発注、在庫管理、売掛金管理は上述)	○		営業秘密情報の保持		○		長時間・頻繁の停止は不可
		金融	地銀向け、信金向け共同アウトソーシング	○		営業秘密情報の保持	○			極めて高い要求レベル

大分類	小分類	サービス種別	サービスの定義	機密性			可用性			
				高	低	理由	高	中	低	理由
			信用情報提供	○		営業秘密情報の保持			○	
		保険業	見積支援(生命保険等)　(CRM は上述)	○		一般個人情報の保持		○		機会損失を生じないことが重要
			見積支援(自賠責保険)	○		一般個人情報の保持			○	
		宿泊業	予約・空室管理 (CRM、ネットショッピングは上述)	○		一般個人情報等の保持		○		機会損失を生じないことが重要
		医療・介護・福祉	電子カルテ	○		一般個人情報の保持	○			常に稼動の必要あり
			レセプト(保険請求含む)	○		一般個人情報の保持	○			常に稼動の必要あり
			診療予約	○		一般個人情報の保持		○		長時間・頻繁の停止は不可
			処方箋サービス		○				○	
			介護業務支援(報告、請求)	○		一般個人情報の保持		○		長時間・頻繁の停止は不可
		公共電子申請	公共機関への電子申請を行うサービス(施設予約を含む)	○		一般個人情報等の保持		○		長時間・頻繁の停止は不可
		電子入札	－	○		営業秘密情報の保持	○			常に稼動の必要あり
		公共住民情報	住民基本台帳に係るサービス　※※このリストに入れても大丈夫でしょうか？	○		一般個人情報の保持	○			常に稼動の必要あり
		公共個別部門業務	図書館システム(個人情報含む)	○		一般個人情報の保持		○		国民の求めるレベルは高い
ASP 型共通サービス	共通アプリケーション	グループウェア	アドレス帳を含む掲示板や情報共有サービス	○		顧客の内部個人情報保持		○		長時間・頻繁の停止は不可
		アドレス帳サービス	アドレス帳単体で提供するサービス	○		一般個人情報の保持		○		長時間・頻繁の停止は不可
		オンラインストレージ	ネットワーク越しにストレージを提供するサービス	○		営業秘密情報等の保持	○			預かるデータを利用するサービスの可用性要求に準ずる。
								○		
									○	
					○		主として可用性中 or 低			
		ワークフロー	業務のワークフロー管理を行うサービス	○		営業秘密情報等の保持	○			ワークフローを設定する業務の可用性要求に準ずる。
								○		
									○	
					○		主として可用性中 or 低			
		Web サイトのホスティング	Web サイトをホスティングするサービス 例：ネットショッピング、電子商取引、乗り換え情報提供サービス　等	○		一般個人情報等の保持	○			電子商取引アウトソーシング等の可用性要求に準ずる
									○	自ら売買するネットショップの可用性要求に準ずる
					○		産地直送サービス、乗換情報提供等の可用性要求レベル			
		ブログ・コミュニティコーディネート	ブログ、コミュニティを構築・運用するサービス	?	?	顧客の利用方法で選択	?	?	?	顧客の利用方法で選択
		アフィリエイト	－	○		一般個人情報の保持			○	
		メール配信	メール配信(DM)	○		一般個人情報の保持			○	
		コンテンツデリバリ、ストリーミング	映像等のコンテンツを効率よく利用者に提供するサービス	?	?	顧客の利用方法で選択	?	?	?	顧客の利用方法で選択
		電話会議、TV 会議、Web 会議	－		○				○	
		乗り換え	公共交通の乗換情報を検索するサービス		○				○	
		GIS(地理情報システム)/GIS 応用	地理情報のみを取り扱うシステム		○				○	
			コンテンツ/アプリケーションを含んだ GIS 応用サービス	?	?	統合対象により判断	?	?	?	統合対象により判断
		不動産物件検索	新築、中古売買、賃貸の情報検索サービス		○				○	
		映像監視	CCTV 映像の監視、解析サービス	?	?	顧客の利用方法で選択	?	?	?	顧客の利用方法で選択

大分類	小分類	サービス種別	サービスの定義	機密性			可用性			
				高	低	理由	高	中	低	理由
	アプリケーション基盤	決済サービス	お金の決済を行う基盤サービス	○		一般個人情報等の保持	○			常に稼動の必要あり
		メディア・言語変換サービス	記録メディアや言語を変換する基盤サービス	?	?	顧客の利用方法で選択	?	?	?	顧客の利用方法で選択
		位置時間証明サービス	居場所と時刻を証明する基盤サービス	○		一般個人情報の保持		○		リアルタイムかつ継続運用が不可欠
		検索サービス	検索機能を提供する一般向けサービス		○				○	
			個別用途の検索機能を提供するサービス	?	?	顧客の利用方法で選択	?	?	?	顧客の利用方法で選択
		認証サービス	電子証明書による認証を提供する基盤サービス	○		一般個人情報等の保持	?	?	?	認証ターゲットにより選択
	セキュリティ基盤	セキュリティサービス	例：ウィルス・スパム対策、フィルタリング対策(大規模)	○		ログ等の秘密情報の保持	○			大量の利用者を持ち、常に稼動を確保する必要あり
			例：安価なウィルス対策(パターンファイル更新管理)		○				○	
		ネットワーク監視	－		○		○			常に稼動の必要あり
		不正アクセス監視	－	○		営業秘密情報の保持	○			常に稼動の必要あり

判定の結果、一部の ASP・SaaS サービスについては、顧客との SLA 契約に応じて求められるレベルが変動する等の要因により、CIA に対する要求レベルを一律に設定するのが困難であることが判明したため、「一律にパターンを設定することが困難なサービス」として整理している。

さらに、各 ASP・SaaS サービスをパターンごとに集約した結果を図表 24 に示す。

図表 24　各パターンに該当する ASP・SaaS サービス

パターン	サービス種別
1	受発注、人事給与・勤怠管理・経理、ERP(財務会計等)、文書管理(個人情報・営業秘密情報含む)、EC サポート(電子商取引のアウトソーシング)、ネットショッピング支援(仮想店舗貸しサービス)、コールセンター支援、金融業特化型 ASP(地銀・信金共同アウトソーシング)、医療・介護・福祉業特化型 ASP(電子カルテ、レセプト)、電子入札、公共住民情報、決済サービス、不正アクセス監視
2	販売管理・売掛金管理、公共窓口業務、在庫管理、建設業特化型 ASP、卸売・小売・飲食業特化型 ASP、保険業特化型 ASP(生命保険見積)、宿泊業特化型 ASP、医療・介護・福祉特化型 ASP(診療予約、介護業務支援)、公共電子申請、公共個別部門業務、グループウェア、アドレス帳サービス、位置時間証明サービス
3	購買支援、CRM・営業支援、販売支援、契約、採用管理、資産管理、e ラーニング・LMS に係る個人情報システム、ネットショッピング(自らの売買支援)、金融業特化型 ASP(信用情報提供)、保険業特化型 ASP(自賠責保健見積)、アフィリエイト、メール配信
4	ネットワーク監視
5	文書管理(個人情報・営業秘密情報を含まず)、EC サポート(産地直送等、物流・決済を一括で提供)
6	広告、IT 資産管理、e ラーニング・LMS、ニュースリリース業務、運輸業特化型 ASP、医療・介護・福祉業特化型 ASP(処方箋サービス)、電話会議/TV 会議/Web 会議、乗り換え、GIS(地図情報のみの取り扱い)、不動産物件検索、検索サービス(一般向け)
※	ブログ・コミュニティコーディネート、コンテンツデリバリー・ストリーミングサービス、GIS 応用サービス(コンテンツ、アプリケーションを含むもの)、映像監視、メディア・言語変換サービス、検索サービス(個別用途)、認証サービス

※一律にパターンを設定することが困難なサービス

なお、今回の類型化作業は、現在提供されている典型的な ASP・SaaS サービスを対象として実施しているため、図表 24 は、すべての ASP・SaaS サービスを網羅しているものではないことに留意する必要がある。

従って、適合する ASP・SaaS サービスが図表 24 中に存在しない場合、又は「一律にパターンを設定することが困難なサービス」に該当する場合においては、先述した CIA に対する要求レベルの判定基準に基づき、パターン１から６までのうち、該当するパターンを独自に判定する必要がある。

【2】 構成要素の特定

ASP・SaaS サービスが持つ情報資産を特定するためには、ASP・SaaS を構成するハードウェア、ソフトウェア、通信機器・回線及び建物等の典型的な構成要素を整理する必要がある。

多種多様な ASP・SaaS サービスが存在することを考慮して、サービス形態に大きく影響する以下の事項に着目した上で 4 つの ASP・SaaS サービス事例を想定し、構成要素の洗い出しを行った。

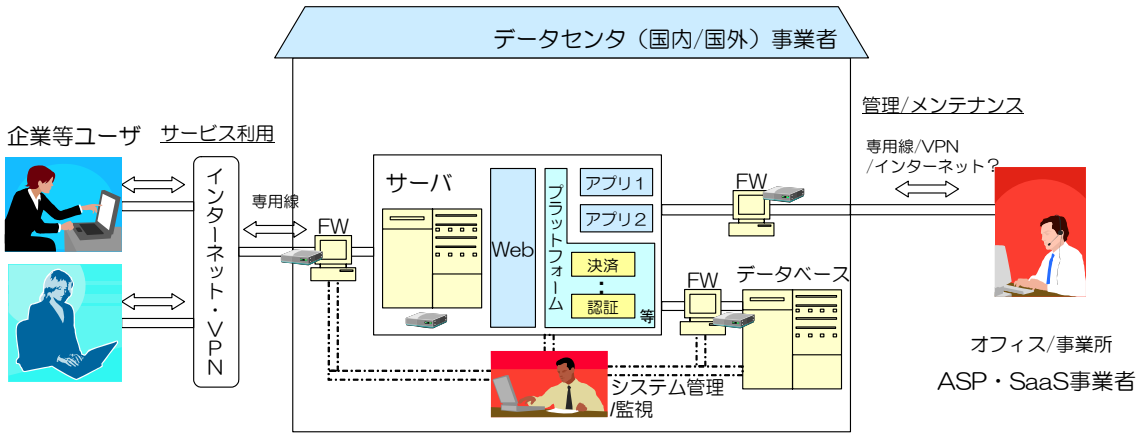
⑴インターネットデータセンタ(IDC)等、外部事業者の活用の有無

⑵他の ASP・SaaS 事業者との業務連携の有無

＜事例１＞ASP・SaaS 事業者が IDC 等の外部事業者を活用する場合

この形態の場合、情報セキュリティ対策(FW、IDS、ログ監視等)を ASP・SaaS 事業者が自ら実施しているか、あるいは外部事業者にアウトソーシングしているかに注意が必要である。なお、サーバ及び FW 等の OS レベル維持管理のみをアウトソーシングしている事例も見受けられる。

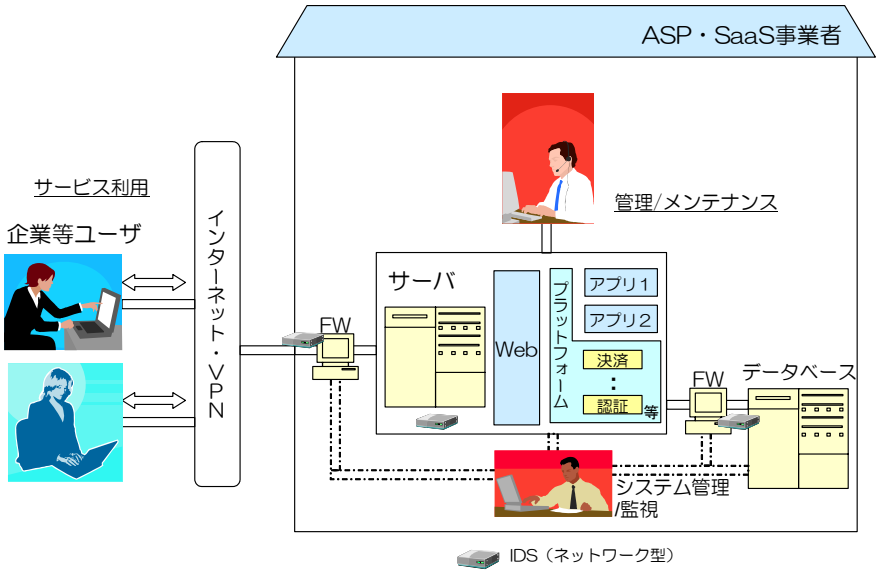
図表 25　ASP・SaaS 事業者が IDC 等の外部事業者を活用



＜事例２＞ASP・SaaS 事業者自らが設備等を維持管理する場合

この形態の場合、ウイルスやサーバ負担分散等の対策として、ISP の提供するアプライアンスサービス等を利用する可能性が想定される。

図表 26　ASP・SaaS 事業者自らが設備等を維持管理

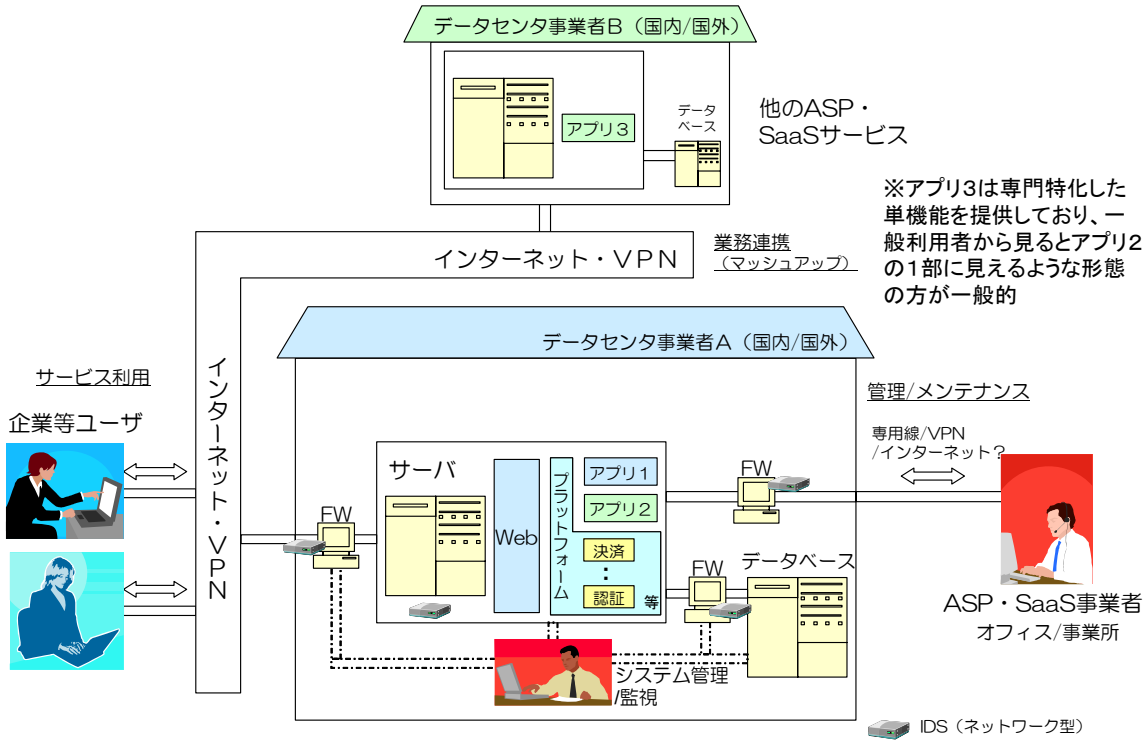


＜事例３＞ASP・SaaS 事業者間の業務連携がある場合①＜サーバ間連携なし＞

事業者間は、インターネット経由の XML メッセージ交換のようなゆるい連携形態を取っている。現在は、この方式が主流である。

この形態の場合、他事業者のアプリケーションは、利用者からは提供を受けている ASP・SaaS 事業者のサービスの一部に見えるのが一般的である。

図表 27　ASP・SaaS 事業者間の業務連携あり・サーバ間連携なし

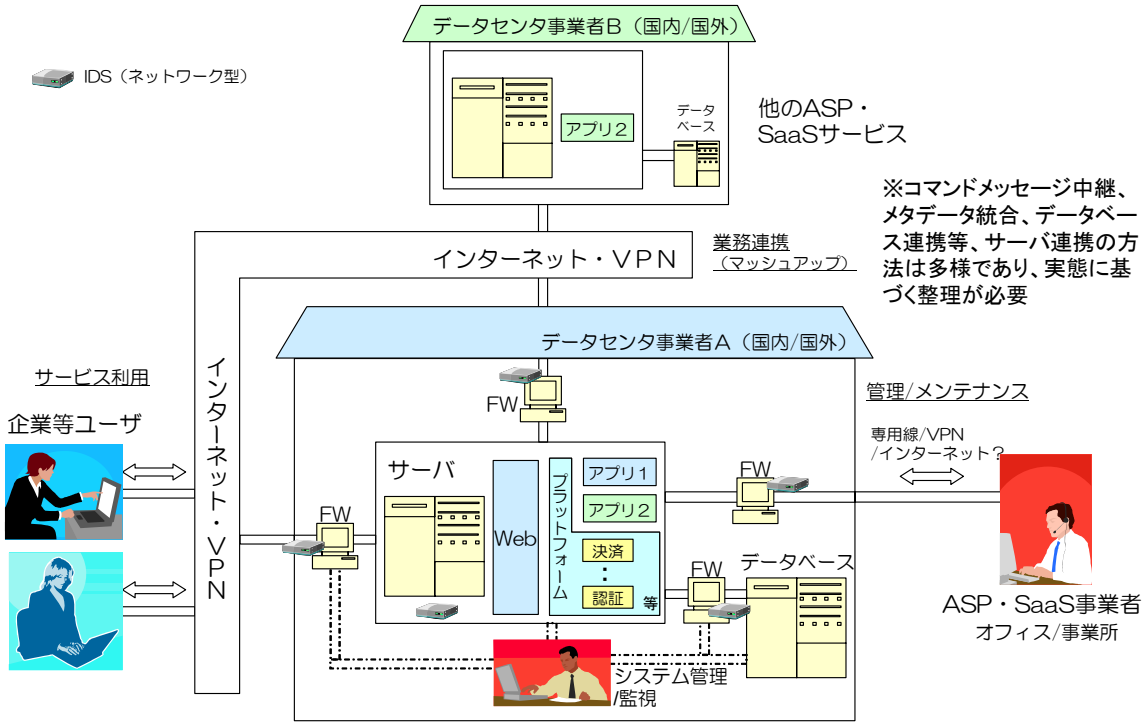


＜事例４＞ASP・SaaS 事業者間の業務連携がある場合②＜サーバ間連携あり＞

事業者間のシステム連携が本格的に実装されているケースである。この場合は事業者間の接続回線は専用線等の高品質サービスが主である。この事例は、事例３の特別ケースと捉えることもできる。

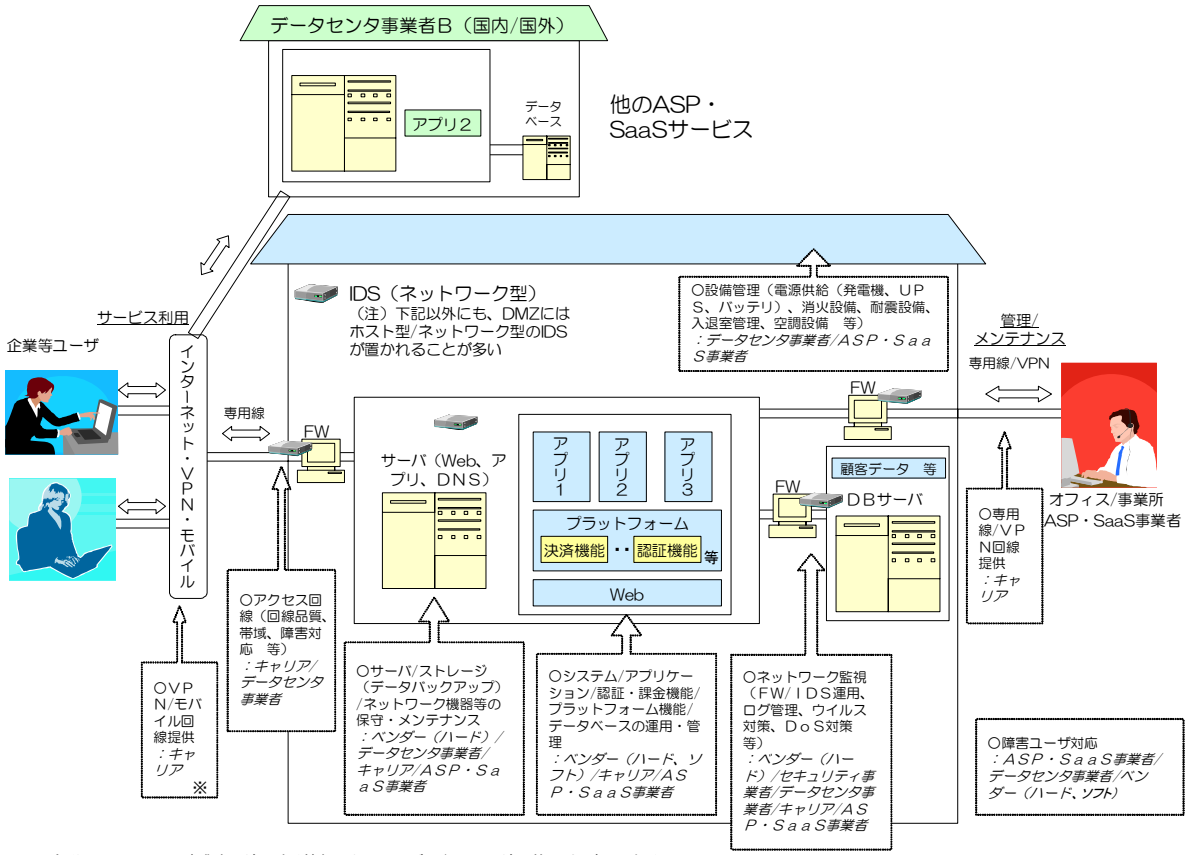
この形態の場合、メタデータ統合及びデータベース連携等、サーバ連携の方法は多様である。

図表 28　ASP・SaaS 事業者間の業務連携あり・サーバ間連携なし



以上の４つの構成事例に基づき、ASP・SaaS の典型的な構成要素を抽出した結果は図表 29 のとおりである。ここでは、事例４は事例３の特別ケースと考え、事例３の事業者連携の形態を「典型的」と捉えて整理している。

図表 29　ASP・SaaS の典型的な構成要素(図)



※この部分は、ASP･SaaS事業者に適用する情報セキュリティガイドラインの適用範囲外と考えられる

次に、構成要素の分類を行う。ASP・SaaS 事業者では、サービス提供における大括りの単位として、まず「データセンタに委託できる建物・電源（空調等）の設備部分」をインフラと位置付けて考え、次に「サービス提供のために外部接続を行うためのネットワーク」が契約実施対象としてあり、さらに事業者のサービスに密着した主として自らの資産である「アプリケーション・プラットフォーム・ストレージ等」があるというとらえ方が広く受け入れられているため、この考え方に則って分類を行う。

この分類方法を採用することにより、ASP・SaaS 事業者は、構成要素を分かりやすくとらえることが可能となり、結果として、各構成要素に対応付けられた対策項目を理解しやすくなる。

上記の観点から構成要素を分類したものを図表 30 に示す。

図表 30　ASP・SaaS の典型的な構成要素(表)

分類	典型的な構成要素
1.アプリケーション、プラットフォーム、ストレージ等	【アプリケーション部分】 ・ASP・SaaS アプリケーション
	【プラットフォーム】 ・ASP・SaaS 事業者が利用するプラットフォーム （例）決済、認証、検索、位置時間証明等
	【サーバ、ストレージ等のハード部分】 ・サーバ群（付随する OS 等の基盤ソフトを含む） ・データベース（付随する OS 等の基盤ソフトを含む） ・ストレージ ・通信機器 ・情報セキュリティ対策機器
2.ネットワーク	・外部ネットワーク
3.建物、電源(空調等)	・建物 ・サーバルーム（サーバ群、データベース等を格納している部屋） ・物理的セキュリティ境界 ・電源 ・空調
4.その他	・運用管理端末 ・保管媒体（紙、磁気メディア、光メディア等）

【3】 構成要素に基づく情報資産の洗い出し

【2】項において抽出・分類した構成要素に基づいて、ASP・SaaS サービスの情報資産の洗い出しを行う。

情報資産とは、情報セキュリティ対策を適用する対象のことであり、今回の検討では、ASP・SaaS の情報資産を、構成要素そのもの及び各構成要素を介する情報と定義する。

この定義に基づき、新たに構成要素を介する情報のリストアップを行い、該当する構成要素にマッピングした上で情報資産としてとりまとめた。なお、各構成要素を介する情報についても、構成要素と同様に典型的なものを想定した。

以上を踏まえ、ASP・SaaS における情報資産のリストアップを実施した結果を図表 31 に示す。

図表 31　ASP・SaaS の構成要素における情報資産(表)

分類	情報資産
1.アプリケーション、プラットフォーム、ストレージ等	【アプリケーション部分】 ・ASP・SaaS アプリケーション&アプリケーションログ(利用、管理) ・サービスデータ（利用者情報） ・サービスデータ（管理者情報）
	【プラットフォーム】 ・ASP・SaaS 事業者が利用するプラットフォーム&ログ(利用、管理) （例）決済、認証、検索、位置時間証明等
	【サーバ、ストレージ等のハード部分】 ・サーバ群（付随する OS 等の基盤ソフトを含む）&サーバログ（利用、管理） ・データベース（付随する OS 等の基盤ソフトを含む）&データベースログ（利用、管理） ・ストレージ&管理ログ ・通信機器&管理ログ ・情報セキュリティ対策機器&管理ログ
2.ネットワーク	・外部ネットワーク
3.建物、電源(空調等)	・建物 ・サーバルーム（サーバ群、データベース等を格納している部屋） ・物理的セキュリティ境界 ・電源 ・空調
4.その他	・運用管理端末 ・保管媒体（紙、磁気メディア、光メディア等）

※アンダーライン部分が構成要素に対して追加された情報そのもの

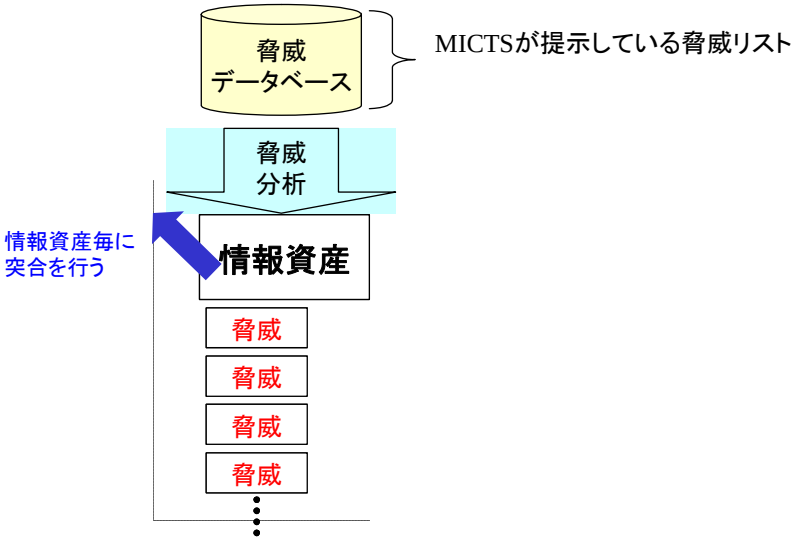
【4】 情報資産に対する脅威分析

【3】項において、ASP・SaaS における情報資産を特定したが、これらの情報資産を保護するために適切な情報セキュリティ対策を導出するためには、情報資産に対してどのような脅威が想定されるかについて分析する必要がある。

なお、脅威の選別にあたっては、情報資産の CIA に直接作用する脅威のみを抽出することとした。例えば、物理的な破壊は、ハードウェアには直接的な脅威として作用するが、電子データには間接的にしか作用しないため（つまり、ハードウェアが破壊されることにより電子データが失われるという対応関係）、ハードウェアに対する脅威としてのみ考慮する。これにより、情報資産を保護するために必要最小限の対策を効率的に導出することが可能となる。

以上を踏まえ、情報資産に対して想定される脅威を抽出するイメージを図表 32 に示した。

図表 32 脅威の突合のイメージ



情報資産に対応する脅威を網羅的に分析するためには、情報セキュリティ分野における一般的な脅威がリスト化されている MICTS を活用するのが効果的である。

今回の検討においては、図表 33 に示す脅威のリストを参照しつつ、各情報資産の CIA に被害を与える可能性がある脅威を抽出した。

図表 33　考えうる脅威のタイプのリスト(抜粋)

脅威が対象とするもの	脅威の分類	脅威の詳細分類
外部の第三者もしくは内部の人間の悪意に起因する脅威を対象とするもの	情報資産の機密性の損失	情報セキュリティ違反、ウイルス感染、不正プログラム実行、情報資産の盗難、情報資産の持ち出し、不正アクセス、許可されていない区域への侵入、情報処理施設や設備の悪用、盗聴
	情報資産の完全性の損失	従業員による情報セキュリティ違反、ウイルス感染、不正プログラム実行、情報資産の盗難、情報資産の不正変更、情報処理施設や設備の破壊
	情報資産の可用性の損失	従業員による情報セキュリティ違反、ウイルス感染、不正プログラム実行、情報資産の盗難、情報処理施設や設備の破壊、情報処理施設や設備の悪用、システムリソースの浪費、サービス不能攻撃、スタッフ不在、障害復旧の妨害
内部の人間の過失に起因する脅威を対象とするもの	情報資産の機密性の損失	情報セキュリティ違反(理解不足に起因)、ウイルス感染、不正プログラムによる被害、情報資産の持ち出し、従業員の操作エラー、システムの誤動作
	情報資産の完全性の損失	情報セキュリティ違反(理解不足に起因) ウイルス感染、不正プログラムによる被害、情報資産の持ち出し、情報資産の変更、事故による情報処理施設や設備の破壊
	情報資産の可用性の損失	情報セキュリティ違反(理解不足に起因)、ウイルス感染、不正プログラムによる被害、情報資産の持ち出し、事故による情報処理施設や設備の破壊、システムの誤動作、システムリソースの浪費 スタッフ不在、障害復旧の遅れ
自然災害等、人的でない要因に起因する脅威を対象とするもの	災害	地震、振動、洪水、台風、落雷、火災、煙
	インフラストラクチャーの障害	通信回線の不安定、電話回線の不安定、電力の不安定
	一般的な環境障害	極端な温度及び湿気、ほこり、電磁波放射
	情報資産の劣化	ハードウェアの劣化、ネットワーク機器の劣化、媒体の劣化、ドキュメントの劣化

出典：MICTS

脅威分析の過程において、ある情報資産に対して抽出される脅威の実例を図表 34 に示す。

図表 34　情報資産「サービスデータ（利用者情報）」に関する脅威

種別	分類	脅威の詳細分類
外部もしくは内部の人間の悪意に起因する脅威	機密性損失	情報セキュリティ違反、不正プログラム実行、情報資産の盗難、情報資産の持ち出し、不正アクセス、盗聴
	完全性損失	従業員による情報セキュリティ違反、不正プログラム実行、情報資産の不正変更
	可用性損失	従業員による情報セキュリティ違反、不正プログラム実行
内部の人間の過失に起因する脅威	機密性損失	情報セキュリティ違反(理解不足に起因)、不正プログラムによる被害、情報資産の持ち出し、従業員の操作エラー
	完全性損失	情報セキュリティ違反(理解不足に起因)、不正プログラムによる被害、情報資産の変更
	可用性損失	情報セキュリティ違反(理解不足に起因)、不正プログラムによる被害
自然災害等、人的でない要因に起因する脅威	災害	―
	インフラ障害	―
	一般的な環境障害	―
	情報資産の劣化	―

（注）例えば、地震によるハードディスク障害の結果としてサービスデータが破壊される場合、ストレージに対する直接の脅威が発現したと考える。換言すれば、ストレージが壊れない対策またはストレージのバックアップ対策があればサービスデータは守られる。このように、地震のケースでは不正アクセス防止のようなサービスデータに直接作用する対策は必ずしも求められておらず、従って、情報資産をサービスデータとしているこの表には「地震」は脅威として含まれていない。

【5】 対策項目の導出

本項では、前項における脅威分析の結果に基づいて、ASP・SaaS の情報資産を保護するために必要な物理・技術面の対策項目を導出する。

(a) 基本的な考え方

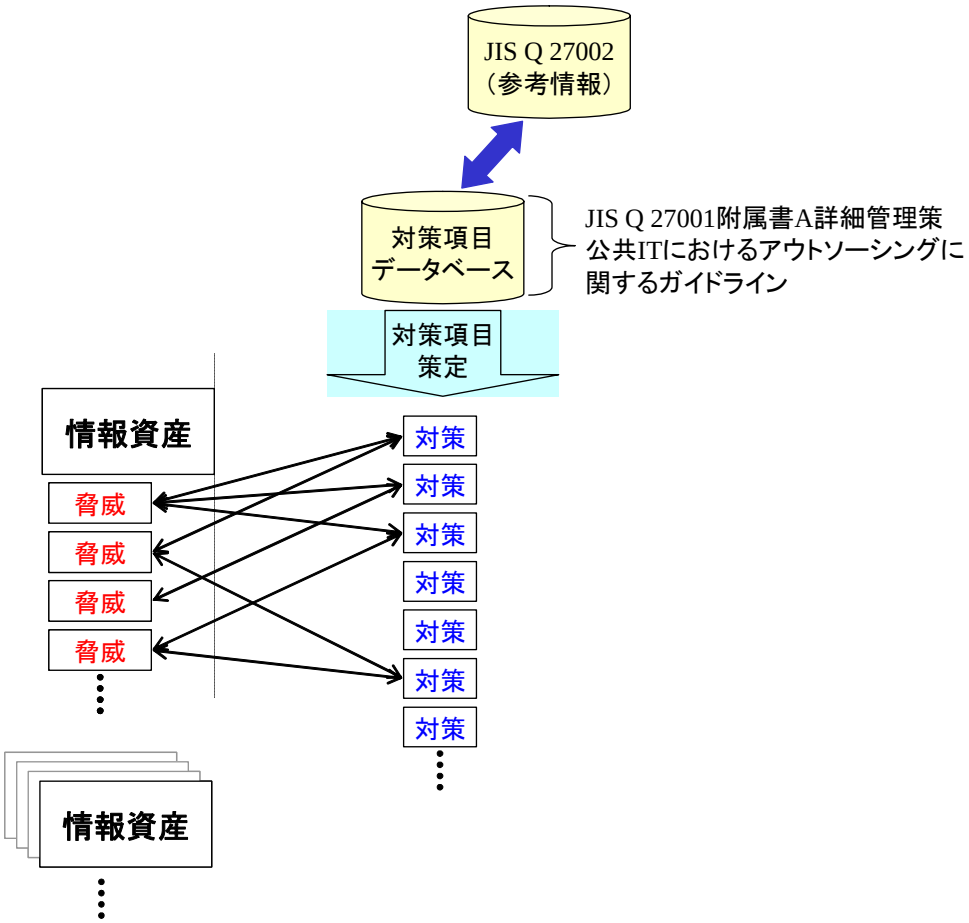
前項までの検討において、ASP・SaaS の構成要素から情報資産を特定し、各情報資産に対する脅威を抽出した。

通常のリスクアセスメントの手順では、情報セキュリティ対策の選別を行うために、さらに情報資産のぜい弱性分析を行って現実のリスクを特定していく。しかしながら、今回の情報セキュリティ対策ガイドラインの策定においては ASP・SaaS サービスの多様性を包含しつつ、これらをカバーする一般的な情報セキュリティ対策を導出しようとしているために、情報セキュリティ対策の具体的な実施状況に基づくぜい弱性の分析を実施することができない。以上のような事情から、ここでは、ASP・SaaS サービスに即した情報資産毎に洗い出された脅威に基づいて、情報セキュリティ対策を直接選別することとする。

本検討における対策項目の選定イメージを図表 35 に示した。ここで、脅威と対策項目の関係は多対多である[12]。

[12] 図上では表れていないが、実際には対策項目は別の情報資産の脅威とも紐付けられることが一般的である。

図表 35 情報セキュリティ対策の導出イメージ



なお、対策項目の導出にあたっては、ASP・SaaS サービスに係る以下のような特有の事情を考慮する。

- 利用者情報等のサービスデータを ASP・SaaS 事業者が一括して預かる
- データに対する完全性の要求が常に高い
- 複数の ASP・SaaS 事業者が連携してサービスを提供する場合、サービス全体の情報セキュリティレベルを調整する必要がある
- サービスの提供・運用・保守のすべてにおいて外部ネットワークが不可欠である
- 外部ネットワークにおいてインターネットが一般的に利用されており、クラッキングや盗聴の対象になりやすい

(b) 対策導出の流れ

以下では、対策選別の処理流れについてまとめる。まず、準備作業として、対策項目の選別を行う際の候補となるデータベースを用意する。

このデータベース準備作業にあたっては、まず非常に網羅性が高い JIS Q 27001 附属書 A の詳細管理策を参考にして、対策項目をリストアップしておく。しかしながら、この段階では、各対策が汎用性が高い分 ASP・SaaS サービスに特化した内容になっていない。次に、対策項目を少しでも ASP・SaaS サービスに特化した内容とするため、ASP・SaaS サービスに特化した情報セキュリティ対策ガイドラインとして実績がある「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」を参考にする。具体的には以下の作業を実施する。

① 「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」が提示している情報セキュリティ対策のうち、民間にも適用可能なものを専門家判断で抽出する
② JIS Q 27001 附属書 A の詳細管理策を参考に作成した汎用性の高い対策項目に対して、①との比較を行い、同じことを言っているものがあれば、より ASP・SaaS の事情に即した①の対策をベースに内容を書き換えていく

以上の準備をした上で、以下の手順で対策項目の選別を実施する。

① 対策項目データベースにある対策が、各情報資産のどの脅威に対して効果があるかを特定する
② ①の紐付け作業により、各対策がカバーすべき情報資産と脅威が明確になるため、必要に応じて JIS Q 27002 も参考にしながら、対策の内容をさらに ASP・SaaS サービスに即した内容に書き換える
③ ①②の作業でカバーされない脅威がないかをチェックし、もしあれば別途対策の必要性と内容を専門家の協力を得て検討する

(c) 対策の分かりやすさの改善

今回策定する情報セキュリティ対策ガイドラインは、基本的には中小企業を多く含む ASP・SaaS 事業者を主要な読み手と想定しているため、内容の読みやすさを重視する必要がある。従って、(b)で選別した対策項目に対してさらに専門家判断を導入し、以下の観点から対策項目の削減と分かりやすさの改善を行った。

- 中小企業にとっても優先的に取り組むべき対策への重点化
- ASP・SaaS サービスにそぐわない表現の書き直し
- 対象が類似する対策を 1 つに集約し、簡潔な表現で実施内容を併記する
- 対策の実施内容が意味的に類似している対策を 1 つに集約し、わかりやすい表現で書き直す
- 複数の情報資産に対して対策の実施内容が同じ場合は、対策は主語が異なるのみと

なっている。これを「共通対策」としてくくりだして集約する。

(d) 対策における「基本」と「推奨」の分類

ここまでに実施してきた対策項目の選別では、ASP・SaaS 事業者に中小企業が多いことから、次のような条件を考慮しながら作業を行っている。

- 企業規模を問わず、実施すべき必要性・重要性が高い対策または実施効果が高い対策は、やりやすさや実施コストに捕らわれず積極的に選別していく
- 中小企業にとっても優先的に取り組むべき対策を重点的に選別する
- 上記に当てはまらない対策についても、ASP・SaaS 特有の事情に合うものは選別していく

この結果、選別された対策の中には、情報セキュリティ対策としての要求レベルが異なるものが混在している。そこで、対策を「基本」と「推奨」に分類することで、対策実施の優先度を示すこととした。各々を分類した際の定義について以下に示す。

「基本」:

ASP・SaaS サービスを提供するにあたり、優先的に実施すべき情報セキュリティ対策のこと。この区分に分類された対策項目は、たとえ直ぐに実施できなくても、できるだけ早い時期に実現を目指すと考えるべきである。

「推奨」:

ASP・SaaS サービスを提供するにあたり、実施することが望まれる情報セキュリティ対策のこと。例えば、他社との差別化や高いユーザ要求への対応を実施する場合に、選択的にこの区分の対策を適用することが考えられる。

なお、組織・運用面の対策項目については、すべてが基本的に全事業者が等しく実施すべき内容と考えられたため、すべての対策項目を「基本」として整理している。

【6】 ベストプラクティスの作成

ASP・SaaS 事業者が対策項目に対する理解を深めることができるように、対策を実施するにあたっての具体的な実施方法や注意すべき点の解説等をまとめたベストプラクティスを対策項目毎に作成した。

ベストプラクティスの作成にあたっては、関連分野の専門家(ASP・SaaS 事業者、情報機器メーカ、ISP 及びデータセンタ事業者等)の知見を積極的に取り入れ、実際の ASP・SaaS サービスの状況に沿った内容及び表現となるよう留意した。また、JIS Q 27002 及び「金融機関等コンピュータシステムの安全対策基準・解説書」(金融情報システムセンター)のベストプラクティスも参考にした。

以下に、物理的・技術的な対策項目に対するベストプラクティスの記述例を示す。

図表 36　物理的・技術的な対策項目に対するベストプラクティスの例

Ⅲ．２．３　サービスデータの保護

Ⅲ．２．３．１【基本】

ユーザのサービス情報、アプリケーション・サーバ等の管理情報やシステム構成情報の定期的なバックアップを実施すること。

【ベストプラクティス】

i. 業務要件、セキュリティ要件等を考慮して、バックアップ方法（フルバックアップ、差分バックアップ等)、バックアップ対象（ユーザデータ、システム情報等)、バックアップの世代管理方法、バックアップの実施インターバル、バックアップのリストア方法等を明確にすることが望ましい。

【7】 パターンに応じた対策実施レベルの設定

【１】項では、ASP・SaaS のサービス種別ごとに異なる CIA 要求に対応できるように、ASP・SaaS サービスを 6 つのパターンに分類した。本項では、当該パターン間で異なる CIA 要求を【5】項において導出した情報セキュリティ対策に対応付けし、多様な CIA 要求を持つ ASP・SaaS サービスに広く適用できる対策集を構築することを目的として、以下の手順により各対策項目に実施レベルを設定した。

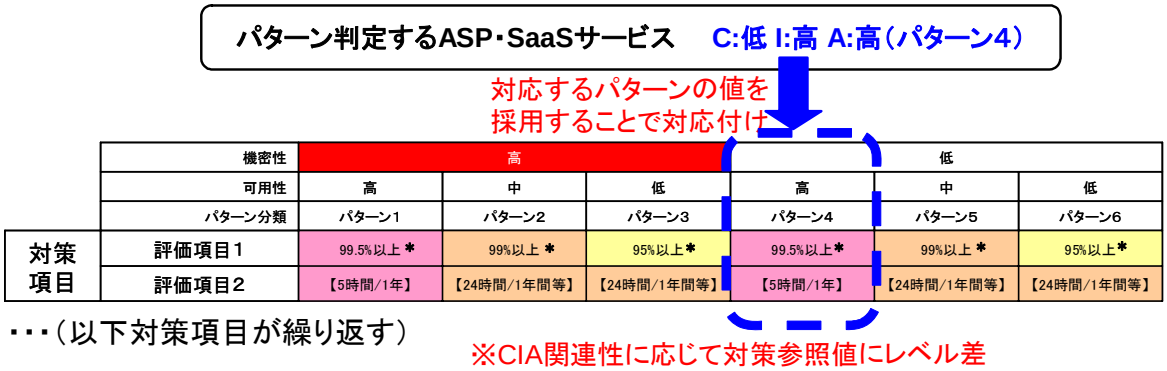
- 各対策項目に対して、「評価項目」を設定する。評価項目は、「対策項目を実施する際に、その実施レベルを定量的あるいは具体的に評価するための指標」と定義する。
- 各評価項目に対して、「対策参照値」を設定する。対策参照値は、「対策項目の実施

レベルの目安となる評価項目の値で、パターンごとに設定する」と定義する。

- 「対策参照値」は、ASP・SaaS 事業者が実施レベルの目安として参照する数値であるが、ASP・SaaS サービスの情報セキュリティ対策を確保する上で、特に達成することが必要と考えられる値については、「＊印」を付した上で、「以上」・「以下」・「以内」等、範囲を限定している。また、ASP・SaaS 事業者が対策参照値を任意で設定可能な場合については、「-」で示している。

各対策項目に実施レベルを設定した結果のイメージを図表 37 に示した。ASP・SaaS 事業者は、提供しているサービスの CIA 要求に合致するパターンを特定し、対応するパターンの対策参照値を採用することで、目指すべき対策実施レベルを容易に導出することができる。

図表 37　ASP・SaaS サービスのパターンと対策実施レベルの対応（イメージ）



なお、評価項目及び対策参照値の設定に際しては、SLA 運用において豊富な実績がある「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」を参照した。

また、関連分野の専門家(ASP・SaaS 事業者、情報機器メーカ、ISP 及びデータセンタ事業者等)の知見を積極的に取り入れることにより、ASP・SaaS サービスの現況との整合性、例えば ASP・SaaS 事業者が実際に対策を行う上での困難性への配慮等について、可能な限り確保するよう留意した。

図表 38 に、対策項目に対して設定した評価項目及び対策参照値の事例を示す。

図表 38　ASP・SaaS サービスのパターン毎の対策参照値の例

【対策項目】

サービス提供に利用するサーバ、プラットフォーム、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性（OS、ミドルウェア、情報セキュリティ対策機器のパッチ等）に関する情報を随時及び定期的に収集し、パッチによる更新を行うこと。

【評価項目】

a.　OS、ミドルウェア、セキュリティ対策機器に対するパッチ更新作業の着手までの時間

パターン	対策参照値
1	ベンダリリースから 24 時間以内*
2	ベンダリリースから 24 時間以内*
3	ベンダリリースから 24 時間以内*
4	ベンダリリースから 3 日以内*
5	ベンダリリースから 3 日以内*
6	ベンダリリースから 3 日以内*

３．３　ガイドラインの特長

３．３．１　ガイドラインの対象範囲

このガイドラインは、ASP・SaaS 事業者が ASP・SaaS サービスを提供する際、実施すべき情報セキュリティ対策全般を対象としている。

ただし、利用者が ASP・SaaS 事業者との契約の範囲外で独自に利用するハードウェア及びソフトウェア（他の ASP・SaaS サービスを含む）、並びに利用者が契約する通信回線及びインターネット・サービスにおける情報セキュリティ対策は対象外である。

３．３．２　ガイドラインの想定読者

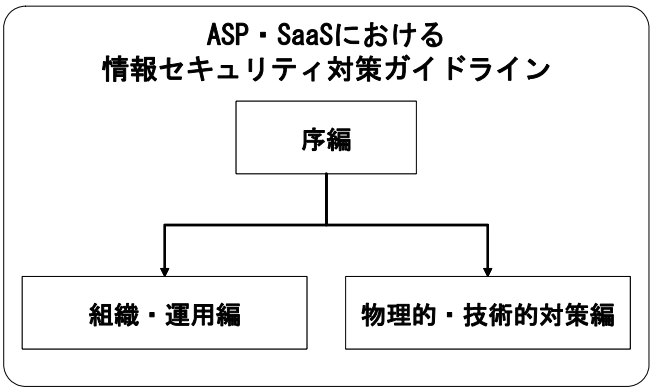
第一には、ASP・SaaS 事業者を想定している。

また、利用者が ASP・SaaS サービスを選定する際に、ASP・SaaS 事業者により実施されている情報セキュリティ対策の状況を確認又は比較対照するための指標として活用することも期待している。

３．３．３　ガイドラインの構成

このガイドラインは、想定読者による積極的かつ幅広い利用を促すため、可能な限り分かりやすく、かつ使いやすいものとすることに留意して作成しており、「序編」、「組織・運用編」及び「物理的・技術的対策編」の３編から構成される。

図表 39　ガイドラインの構成(全体像)



【1】 序編

このガイドラインの目的、対象とする範囲、利用方法・注意事項及び用語の定義等を取りまとめており、「組織・運用編」及び「物理的・技術的対策編」を有効に活用するための導入編として、すべての読者に最初に参照されることを想定している。

【2】 組織・運用編

情報セキュリティを確保するために求められる運用管理体制、外部組織との契約における留意事項及び利用者に対する責任等、組織・運用に係る情報セキュリティ対策を取りまとめており、主として、経営者等の組織管理者によって参照されることを想定している。

以下に、組織・運用編の構成を図示する。

図表 40　組織・運用編の構成

Ⅱ.１ 情報セキュリティへの組織的取組の基本方針
Ⅱ.１.１ 組織の基本的な方針を定めた文書

Ⅱ.２ 情報セキュリティのための組織
Ⅱ.２.１ 内部組織
Ⅱ.２.２ 外部組織（データセンタを含む）

Ⅱ.３ 連携ASP・SaaS事業者に関する管理
Ⅱ.３.１ 連携ASP・SaaS事業者から組みこむASP・SaaSサービスの管理

Ⅱ.４ 情報資産の管理
Ⅱ.４.１ 情報資産に対する責任
Ⅱ.４.２ 情報の分類
Ⅱ.４.３ セキュリティ方針及び要求事項の順守、点検及び監査

Ⅱ.５ 従業員に係る情報セキュリティ
Ⅱ.５.１ 雇用前
Ⅱ.５.２ 雇用期間中
Ⅱ.５.３ 雇用の終了又は変更

Ⅱ.６ 情報セキュリティインシデントの管理
Ⅱ.６.１ 情報セキュリティインシデント及びぜい弱性の報告

Ⅱ.７ コンプライアンス
Ⅱ.７.１ 法令と規則の遵守

Ⅱ.８ サービスサポートの責任
Ⅱ.８.１ 利用者への責任

【3】 物理的・技術的対策編

ASP・SaaS サービスの典型的な要素(アプリケーション、プラットフォーム、ハードウェア、ネットワーク及び建物・電源(空調等)等)における情報資産に対する情報セキュリティ対策を取りまとめており、主として、実際に ASP・SaaS サービスを運用する現場の技術者等によって参照されることを想定している。

以下に、物理的・技術的対策編の構成を図示する。

図表 41　物理的・技術的対策編の章立て

Ⅲ. 1　アプリケーション、プラットフォーム、ハードウェア、ネットワークに共通する情報セキュリティ対策
Ⅲ. 1. 1　運用管理に関する共通対策

Ⅲ. 2　アプリケーション、プラットフォーム、ハードウェア、サービスデータ
Ⅲ. 2. 1　アプリケーション、プラットフォーム、ハードウェアの運用・管理
Ⅲ. 2. 2　アプリケーション、プラットフォーム、ハードウェアのセキュリティ対策
Ⅲ. 2. 3　サービスデータの保護

Ⅲ. 3　ネットワーク
Ⅲ. 3. 1　外部ネットワーク(利用者、管理者、連携ASP・SaaS事業者)からの不正アクセス防止
Ⅲ. 3. 2　外部ネットワーク(利用者、管理者、連携ASP・SaaS事業者との接続)におけるセキュリティ対策

Ⅲ. 4　建物、電源(空調等)
Ⅲ. 4. 1　建物の災害対策
Ⅲ. 4. 2　電源・空調の維持と災害対策
Ⅲ. 4. 3　火災、逃雷、静電気からサービス提供用機器を防護するための対策
Ⅲ. 4. 4　建物のセキュリティ対策

Ⅲ. 5　その他
Ⅲ. 5. 1　機密性・完全性を保持するための対策
Ⅲ. 5. 2　事業者の運用管理端末のセキュリティ
Ⅲ. 5. 3　媒体の保管と廃棄

３．３．４　ガイドラインの利活用方法

このガイドラインは、ASP・SaaS 事業者が、提供するサービス種別に即して分類したパターン毎に適切な情報セキュリティ対策が実施できることを目的としている。

ここでは、ガイドラインの利用対象者別に利用手順の例を示す。

【１】経営者等の組織管理者

i. 「序編」を読み、本ガイドラインの位置付け、利用方法及び用語の定義等を確認する。

ii. 「組織・運用編」に示す情報セキュリティ対策を実施する。対策を実施する際には、必要に応じてベストプラクティスを参照する。

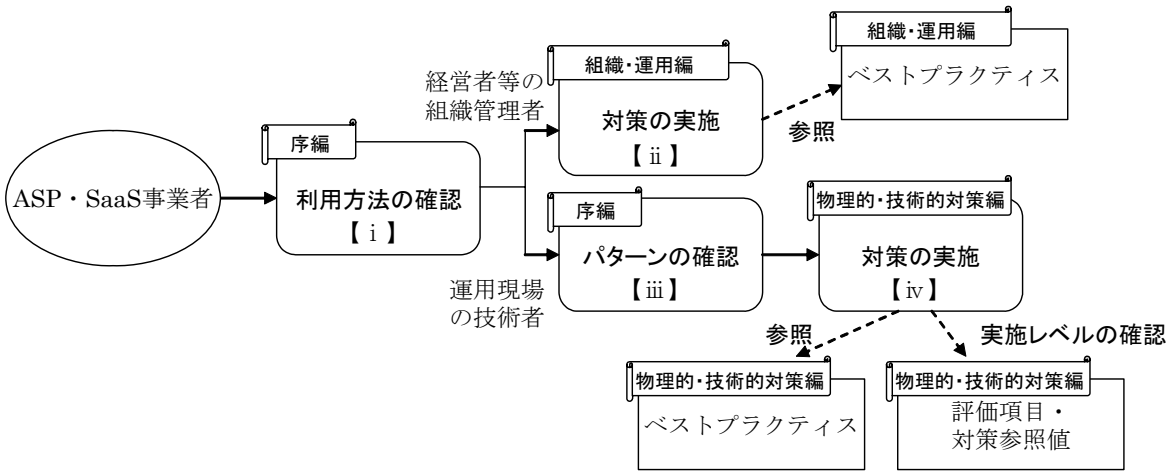
【２】運用現場における技術者等

i. 「序編」を読み、本ガイドラインの位置付け、利用方法及び用語の定義等を確認する。

ii. 「序編」に基づき、自らが提供する ASP・SaaS サービスがどのパターンに該当するかを確認する。

iii. 「物理的・技術的対策編」を見て、自分のパターンに該当する対策を実施する。「基本」の対策から優先的に実施し、さらに「推奨」の対策を実施することが望ましい。なお、対策を実施する際には、必要に応じてベストプラクティスを参照する。また、評価項目を使用し、対策参照値を目安に対策の実施レベルを判断することができる。

図表 42　利用手順(イメージ)



３．３．５　ガイドラインの利活用にあたっての留意事項

ガイドラインの効果的な利用を実現するためには、以下の事項に留意する必要がある。

- **ASP・SaaS サービスの実情に合わせて対策を講じる必要がある場合**

  ガイドラインには、ASP・SaaS 事業者が、提供するサービス内容に即した適切な情報セキュリティ対策を実施するための指針として、可能な限り分かりやすく、かつ具体的な対策項目を提示している。よって、このガイドラインをそのまま利用することで、比較的簡単に ASP・SaaS 事業者が自ら提供するサービスに即した情報セキュリティ対策が実施できると考えられる。

  しかしながら、利用者との契約(SLA)において、より厳しい対策を設定し実施する等、対策レベルの調整を求められる場合は、ガイドラインが示す対策のみにとらわれず、各 ASP・SaaS サービスの実情に合わせて必要な情報セキュリティ対策を講じる必要がある。

- **１の ASP・SaaS 事業者が複数の ASP・SaaS サービスを提供している場合等**

  このガイドラインは、１の ASP・SaaS 事業者が１の ASP・SaaS サービスを提供する場合を基本としているが、１の事業者が複数のサービスを提供する場合には、各 ASP・SaaS サービスを提供するそれぞれの担当部署等の主体が、ガイドライン中の「ASP・SaaS 事業者」にあたるとみなす必要がある。

  また、ASP・SaaS 事業者が、複数の ASP・SaaS サービスにより情報資産を共有している場合で、かつ該当するサービス・パターンが異なる場合は、共有情報資産の保護のため、各パターンの情報セキュリティ対策の中から最も高いレベルのものを選択する必要がある。

第４章　　情報セキュリティ対策ガイドラインの利活用効果と今後の課題

４．１　　ガイドラインの利活用により期待される効果

以下に挙げるガイドラインの利活用効果により、ASP・SaaS 業界全体の情報セキュリティレベルの底上げ、利用者も含めた情報セキュリティに対する意識向上が図られ、ASP・SaaS サービス業界の活性化と健全な発展が期待できると考えられる。

４．１．１　　ASP・SaaS 事業者の視点

ASP・SaaS 事業者にとって期待される効果として以下の４つの事項が想定される。

【１】ASP・SaaS 事業者による適切な情報セキュリティ対策実施の促進

これまで既存の基準・ガイドラインでは困難であった、ASP・SaaS 事業者及びサービスの特性に即した適切な情報セキュリティ対策の促進を図ることができる。

【2】中小・新規参入事業者の情報セキュリティ対策の取り組みの促進

情報セキュリティ対策に人的・金銭的な資源を割くことが困難な中小の ASP・SaaS 事業者や新規参入事業者に対して、個々に対策導出を行う負担を軽減し、優先的に取り組むべき対策の指針を提供することにより、情報セキュリティ対策への取り組みの促進を図ることができる。

【３】連携 ASP・SaaS 事業者に対する情報セキュリティ要求事項の指針として活用

他の ASP・SaaS サービスと連携する際、連携 ASP・SaaS 事業者に対する情報セキュリティ対策の要求事項としてガイドラインが一定の指針となり、ASP・SaaS 特有の事情であるサービス連携におけるトータルな情報セキュリティレベルの向上を期待することができる。

【４】利用者に対する情報セキュリティ対策実施状況の提示内容の指針として活用

ガイドラインの対策項目に沿って情報セキュリティ対策状況を利用者に提示することによって、利用者がその ASP・SaaS 事業者の情報セキュリティレベルを合理的な基準で判断可能となることにより、ASP・SaaS 事業者による情報セキュリティ対策への積極的な取り組みへの動機付けにつながることが期待できる。

４．１．２　　ASP・SaaS サービス利用者の視点

ASP・SaaS サービスの利用者にとって期待される効果として以下の事項が想定される。

【１】ASP・SaaS 事業者の情報セキュリティ対策実施状況の妥当性を、利用者が評価する際の指針として活用

ガイドラインは、利用者が ASP・SaaS サービスを選択するにあたって、ASP・SaaS 事業者が実施している情報セキュリティ対策を評価する際の一定の指針としてなり得る。これにより情報セキュリティレベルとサービス提供価格のバランス感の判断材料としてガイドラインが活用されることを期待できる。

４．２　　今後の課題

４．２．１　　ガイドラインの普及促進

今後、本ガイドラインが ASP・SaaS 事業者における情報セキュリティ対策の指針として、広く普及・活用されるためには、ASP・SaaS 業界における以下のような取組の実施が期待される。

【1】ガイドラインの積極的な活用

ASP・SaaS 事業者の対策実施のガイドラインとしてのみでなく、利用者との契約における SLA の設定基準として活用したり、本ガイドラインに沿った形で自らが実施している情報セキュリティレベルを公表する等、ASP・SaaS 業界における積極的な活用、およびそれによるガイドラインの認知拡大が期待される。

【2】ASP・SaaS の利用環境の変化に対応した見直し・改善

近い将来、技術の進化や新たな ASP・SaaS サービスの登場等の ASP・SaaS サービス及び事業者を取り巻く環境の変化に伴い、本ガイドラインにおける対策が陳腐化し、ASP・SaaS サービス及び事業者の実態にそぐわなくなることが予想される。そのため、ASP・SaaS 業界において、適宜本ガイドラインの見直しを行い、継続的に改善が実施される体制を構築することが期待される。