資料5－4

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～

（最終案）

ＡＳＰ・ＳａａＳの情報セキュリティ対策に関する研究会

平成　　年　　月　　日

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、「経済財政改革の基本方針 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[3]対応等の面で大きなメリット

---

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」

3 情報通信技術を目的に応じて活用するために必要とされる知識や技能のこと。

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[4]（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[5]。

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。

---

[4] 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 140 社(平成 20 年 1 月現在)。

[5] 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。

削除：3
削除：19
削除：0

(c) 課金

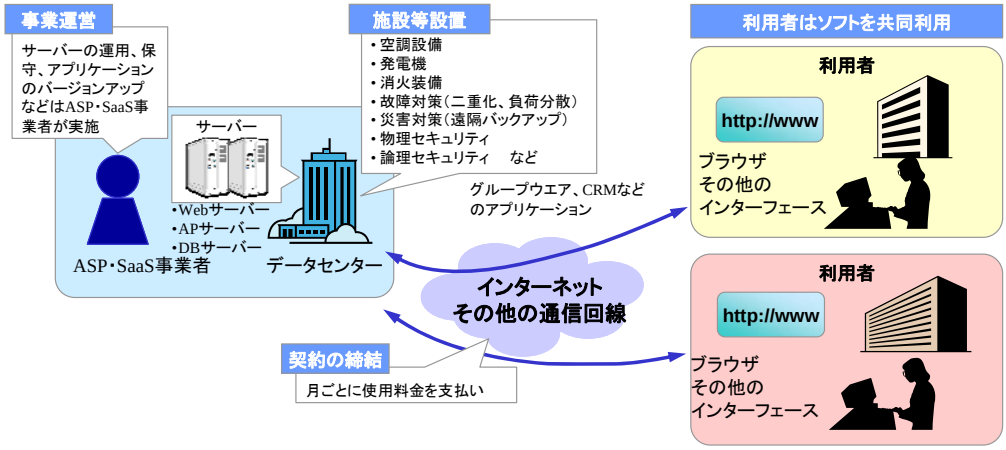
通常のパッケージソフトウエアでは、購入時に一括してライセンス料を支払うことが多い。一方で、ASP・SaaS サービスの場合は、使用時間等に応じて、定期的に使用料金を支払うことが一般的である。

(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。

削除：2005 年を挟んだ

図表 ２　ASP・SaaS サービスにおける技術等の進歩

	従来 （1998～2004 年頃）		新たに加わった技術等 （2005 年頃～）
ネットワークと端末	専用線／インターネット／PC／その他	±	モバイル／電子タグ／その他
対象顧客	BtoC(対個人)／BtoB(法人)／BtoG(公共)／GtoG(公共対公共)		GtoGtoC
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
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
ユーザのカスタマイズ	個別プログラムの変更		メタデータの採用[6]等
他のアプリケーション／サービスとの連携	個別連携		連携用 API を公開等

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

削除：

削除：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

[6] ユーザによるカスタマイズ情報を記録したデータ。アプリケーション・プログラムは、メタデータを使用してカスタマイズされた機能をユーザに提供するため、ASP・SaaS 事業者は、アプリケーション・プログラムそのものをユーザごとにカスタマイズする必要がない。

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[7]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[8]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[9]が主流になり、実装にはバーチャライジング[10]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

削除：[11]

挿入：[11]

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。

---

7 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。

8 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。

9 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。

10 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。

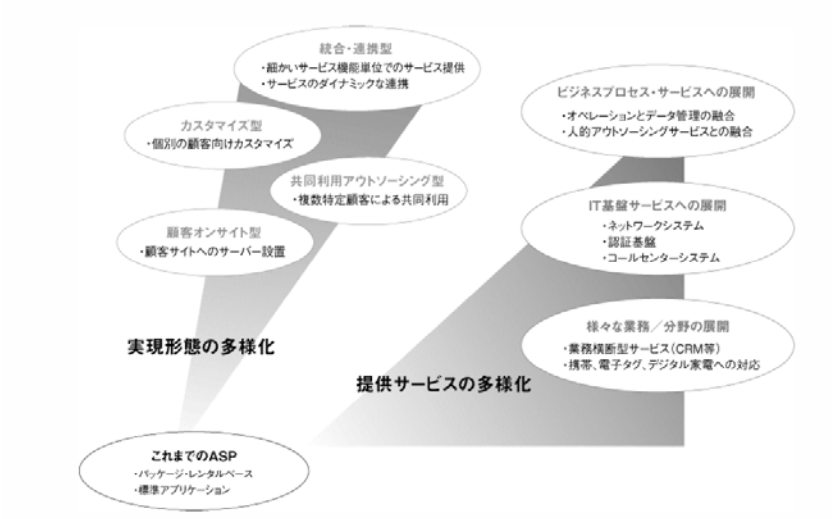
12 2006 年 6 月に成立した「金融商品取引法」の一部規定部分を指す通称。財務報告の適正性を確保するために、上場企業に対して内部統制の構築を義務付けている。

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

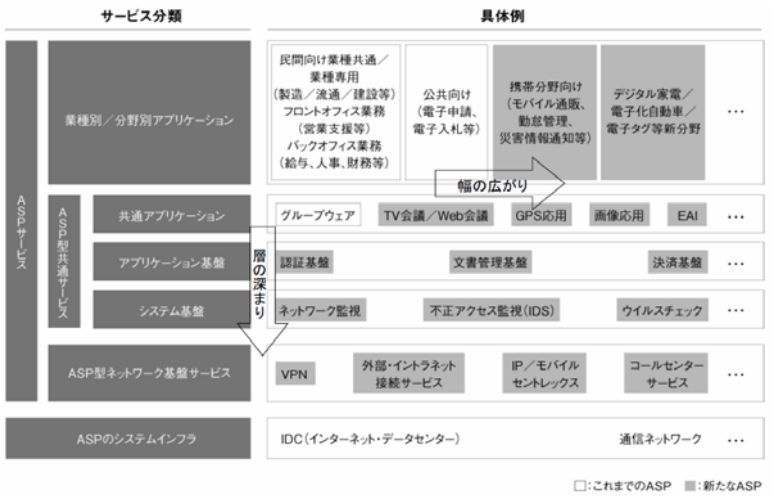
実現形態の面では、前述した異なるアプリケーション同士の「統合・連携型」や、個々の利用者ごとにアプリケーションをカスタマイズして提供する「カスタマイズ型」、地方自治体等に見られる複数の特定顧客による「共同利用アウトソーシング型」、利用者側にサーバ等の機器を設置する「顧客オンサイト型」等、従来に比べその実現形態は様々な広がりを見せている。

(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



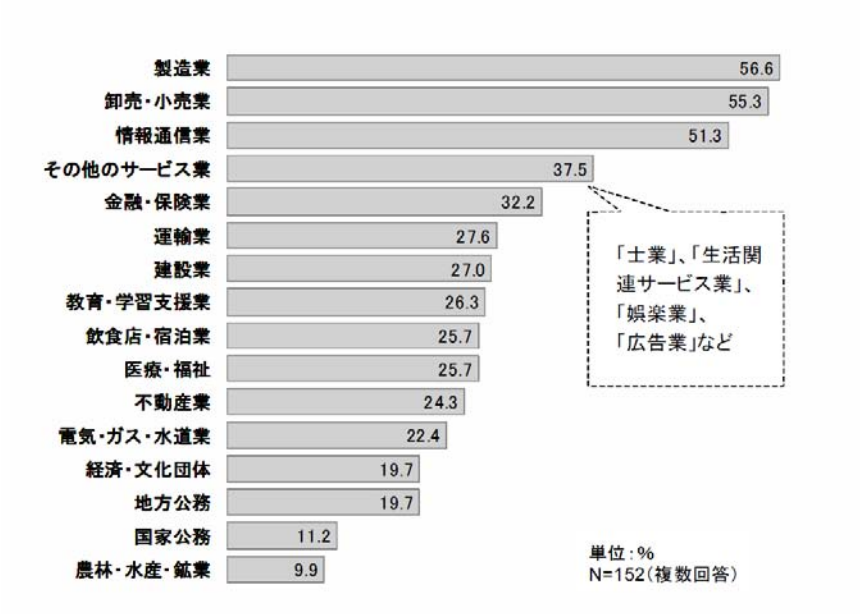
出典：2005 年 ASP 白書 ASPIC Japan／マルチメディア振興センター

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

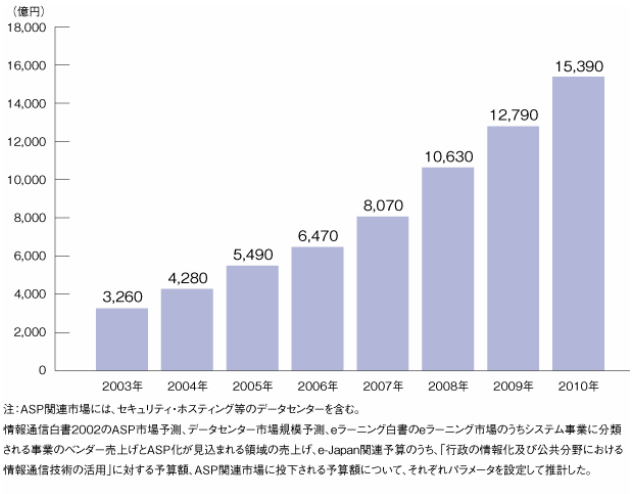
１．４．１　ASP・SaaS サービスの市場規模の推移

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。

削除：.

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



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年に「個人情報の保護に関する法律」が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・

削除：の

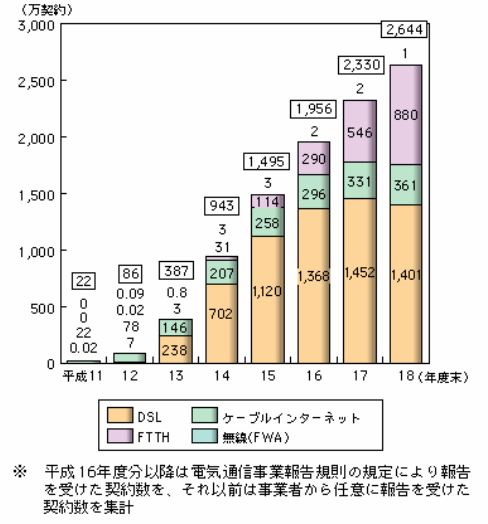
削除：の

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[12]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。

(c) 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



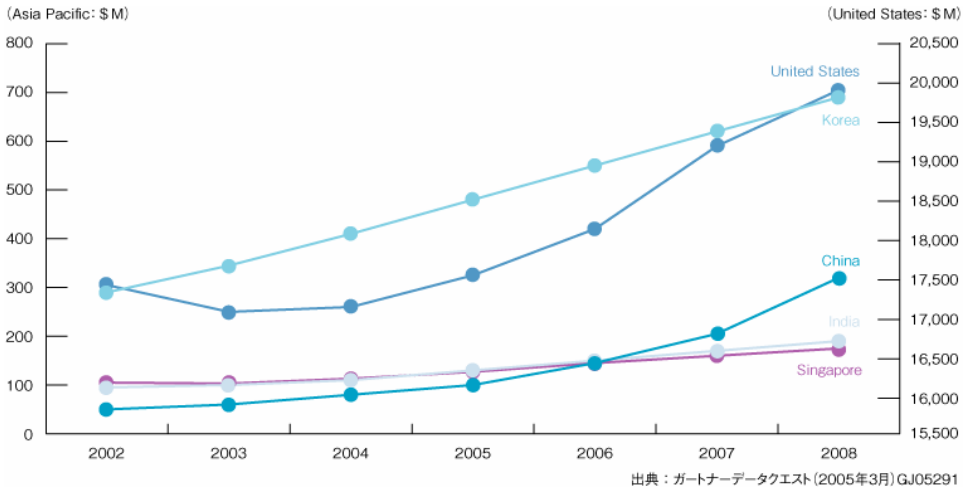
※　平成16年度分以降は電気通信事業報告規則の規定により報告を受けた契約数を、それ以前は事業者から任意に報告を受けた契約数を集計

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



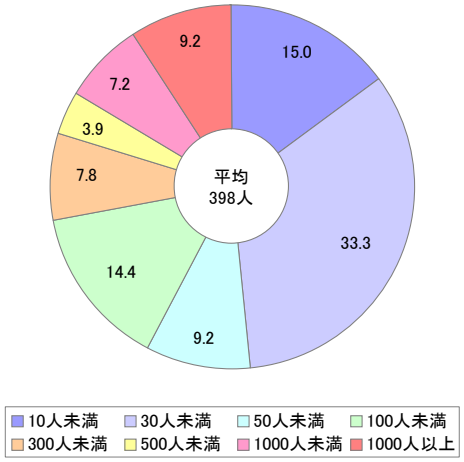
出典：第１回会合資料より抜粋

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、建設業や金融業のような特定の業種に特化した ASP・SaaS サービスや、CRM[13]や ERP[14]といった業務・組織を横断して利用できる ASP・SaaS サービスの提供が進展していることが伺える。

[13] Customer Relationship Management。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。

削除：の略号

[14] Enterprise Resource Planning。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。

削除：の略号

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[15]	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
- 建設業や金融業などの、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

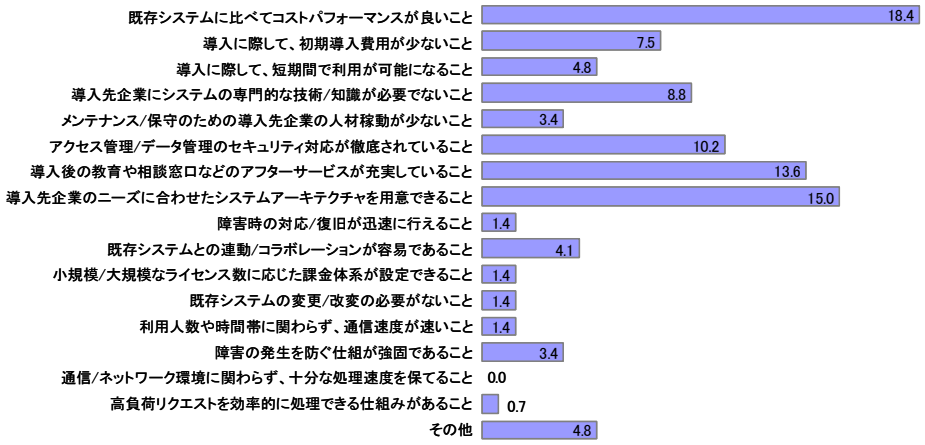
[15] Electronic Data Interchange。商取引に関する情報を標準的な書式に統一することで、企業間での電子的なデータ連携を実現する仕組みを指す。

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対策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 請願・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、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。

(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

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。

(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

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。

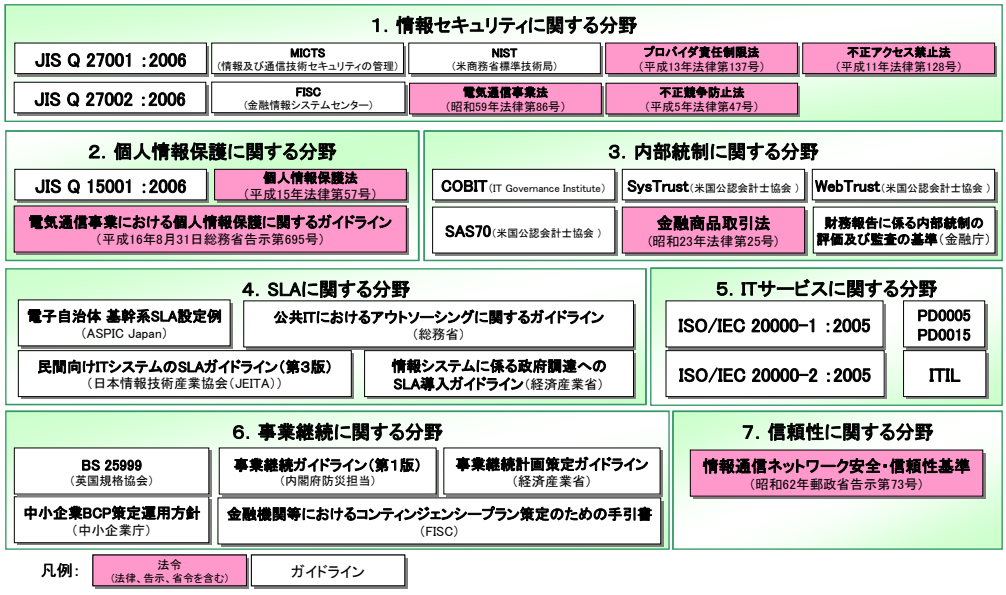
２．２　　現状と課題を踏まえた解決策

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[16]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[17]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。

---

[16] Information Security Management System。企業や組織が自身の情報セキュリティを確保・維持するために、セキュリティポリシーに基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのこと。ISMS の認証取得には、組織全体が日本工業規格「JIS Q 27001」のすべての要求事項に適合していることなどが求められる。

[17] プライバシーマーク。日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定する制度。認定企業は、その旨を示すプライバシーマークを事業活動に関してプライバシーマークの使用を認められる。

(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。

(c) 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インターネット・データセンタ(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

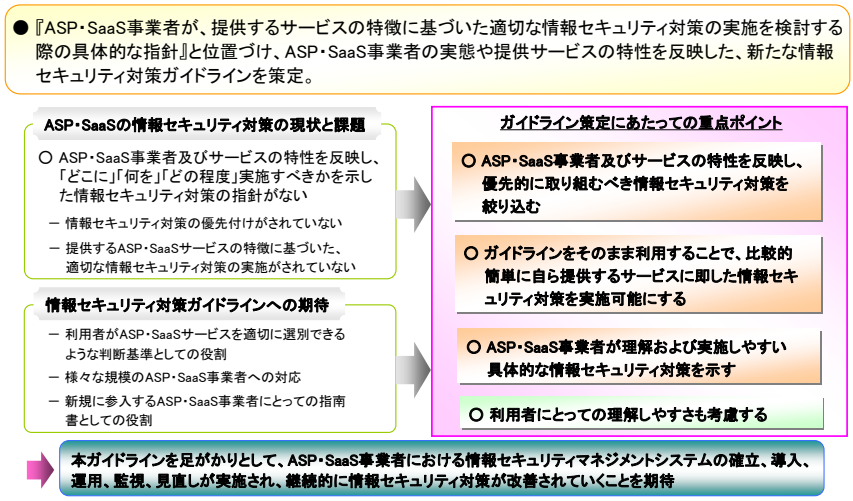
- 他の ASP・SaaS サービスと連携する際、連携 ASP・SaaS 事業者に対する情報セキュリティ対策の要求事項として、本ガイドラインが一定の指針となり得る

- 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

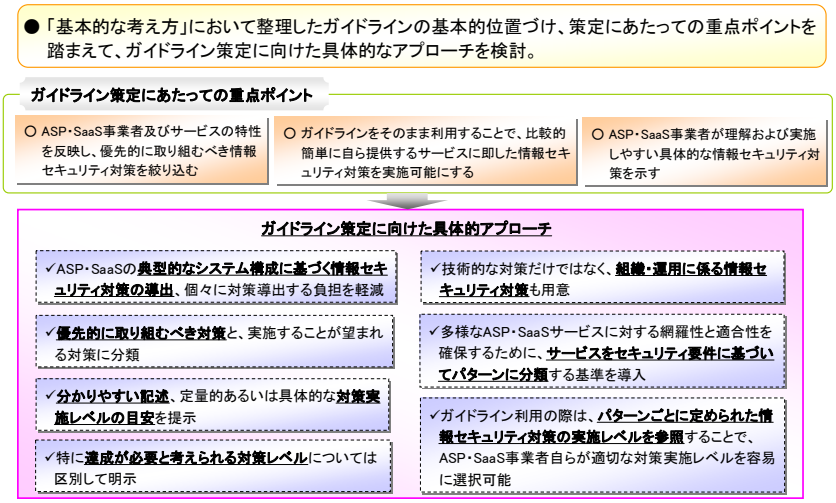
これらの各効果によって、ASP・SaaS 業界全体における情報セキュリティレベルの底上げ、利用者も含めた情報セキュリティに関する意識向上を期待することができる。

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

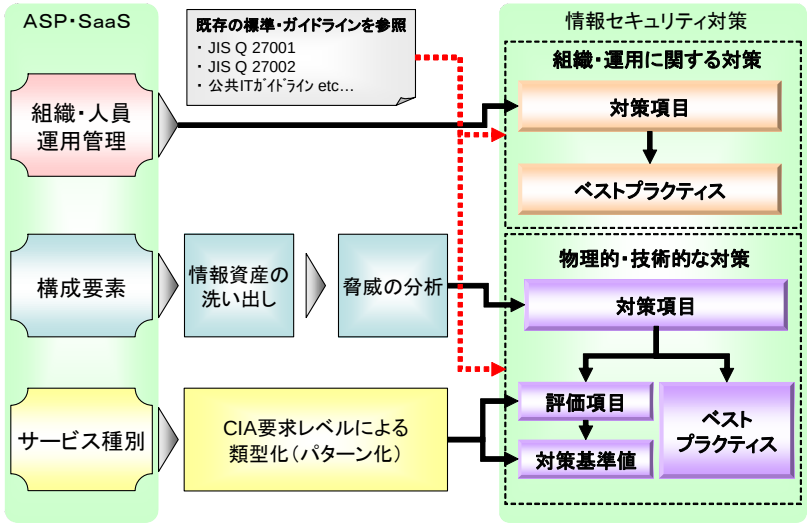
３．２．１　検討の進め方

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
- ユーザサポート責任

削除：サービス

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)
- JIS Q 13335-1:2006（MICTS-1）
- MICTS-2[19]
- 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
- 財団法人 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 第７版

削除：ISO/IEC 27005 [18]（

削除：）

[19] ISO/IEC 27005 として規格化される予定。

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

種別	ステークホルダ	要員
内部組織	ASP・SaaS 事業者	経営者等
		管理責任者、その他の管理者
		それ以外の従業員
		ユーザサポート組織（オペレータ、サポート技術者）
		雇用予定者、雇用変更者、雇用終了者
外部組織	連携 ASP・SaaS 事業者	二
	その他の外部組織	データセンタ、SE 等
二	サービス利用企業	サービス利用者
		利用者の管理連絡窓口

削除：ー

【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[20]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

[20] 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。

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 2O 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。

削除：2

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) ユーザサポートの責任

削除：サービス

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

削除：サービス

【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、インターネット・サービス・プロバイダ(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 事業者から組み込む 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 ASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携 ASP・SaaS 事業者によって確実に実施されることを担保すること。

【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、情報セキュリティに係る取決めを連携 ASP・SaaS 事業者が確実に実施するように、契約や SLA を締結することが望ましい。

ii. 連携 ASP・SaaS 事業者の提供するサービス内容が、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 SLA を締結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「中」程度のサービス

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「中」程度のサービス

【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」[21]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「中」程度のサービス

【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	高	高
2	高	高	中
3	高	高	低
4	低	高	高

[21]本報告書では、一定の条件に合致するかどうかを示す相対的な見出しとして「低」という表現を用いているが、これは情報セキュリティ要求レベルが絶対的に低いことを示すものではない。

5	低	高	中
6	低	高	低

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	診療予約・介護業務支援等、医療・介護・福祉事業の業務プロセスを支援するサービス	○		一般個人情報の保持	○			常に稼動の必要あり
		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	○		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する。
								○		
									○	
					○		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する。
								○		
									○	
					○		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する
									○	自ら売買するネットショップの可用性要求に準する
					○		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
	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		○				○	

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
			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）、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、金融業特化型サービス（地銀・信金共同アウトソーシング）、医療・介護・福祉業特化型サービス、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、建設業特化型サービス、卸売・小売・飲食業特化型サービス、保険業特化型サービス（生命保険見積）、宿泊業特化型サービス、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（顧客管理）・営業支援、販売支援、契約、採用管理、資産管理、ネットショッピング（自らの売買支援）、金融業特化型サービス（信用情報提供）、保険業特化型サービス（自賠責保険見積）、アフィリエイト、メール配信
4	ネットワーク監視
5	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、ニュースリリース業務、運輸業特化型サービス、電話会議・TV 会議・Web 会議、乗り換え、不動産物件検索、検索サービス（一般向け）
※	e ラーニング・LMS、文書管理、オンラインストレージ、ワークフロー、Web サイトのホスティング、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（地図情報システム）/GIS 応用、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、セキュリティサービス

削除：ASP
削除：ASP
削除：（電子カルテ、レセプト）
削除：ASP
削除：ASP
削除：ASP
削除：ASP
削除：医療・介護・福祉特化型 ASP（診療予約、介護業務支援）、
削除：ASP
削除：ASP
削除：ASP
削除：医療・介護・福祉業特化型 ASP（処方箋サービス）、

※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。

(1)IDC 等、外部事業者の活用の有無
(2)他の ASP・SaaS 事業者との業務連携の有無

削除：インターネットデータセンタ(

削除：)

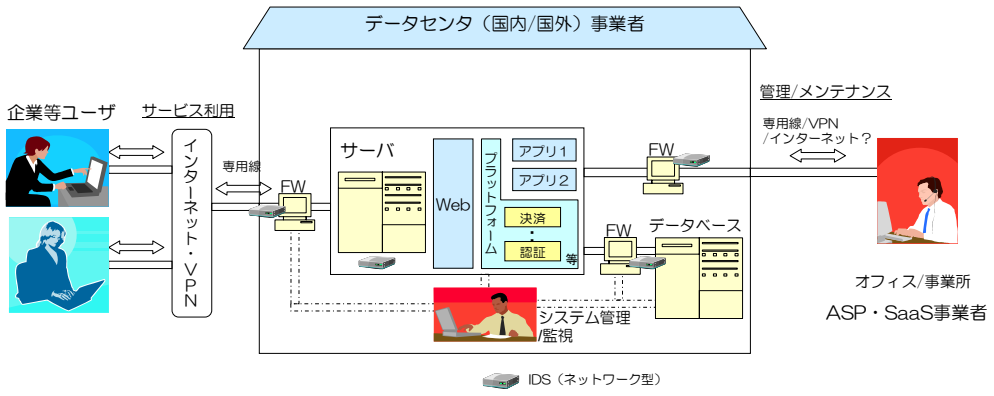
＜事例 1 ＞ASP・SaaS 事業者が IDC 等の外部事業者を活用する場合

この形態の場合、情報セキュリティ対策(ファイアウォール、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、サーバ及びファイアウォール等の 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。

削除：FW

削除：FW

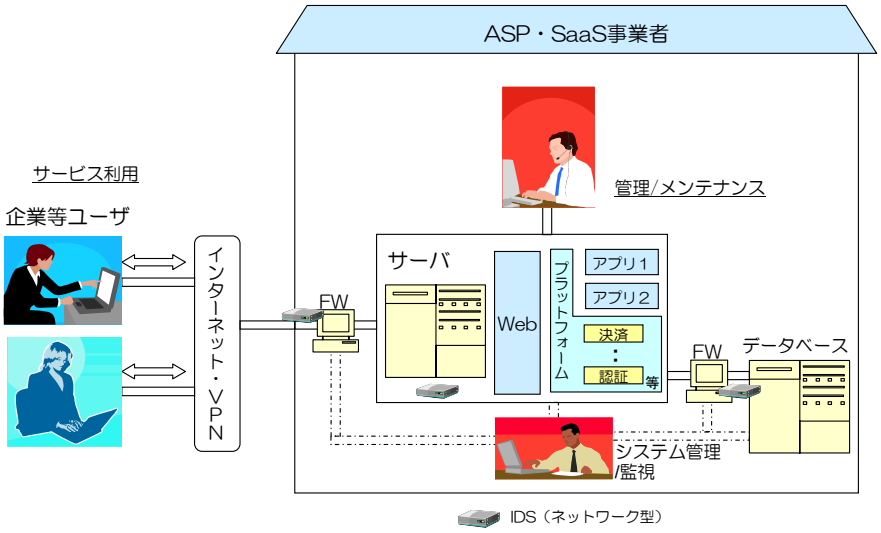
図表 25　ASP・SaaS 事業者が IDC 等の外部事業者を活用



＜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[22]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



[22] ある特定の機能に特化したサービス。

削除：特定

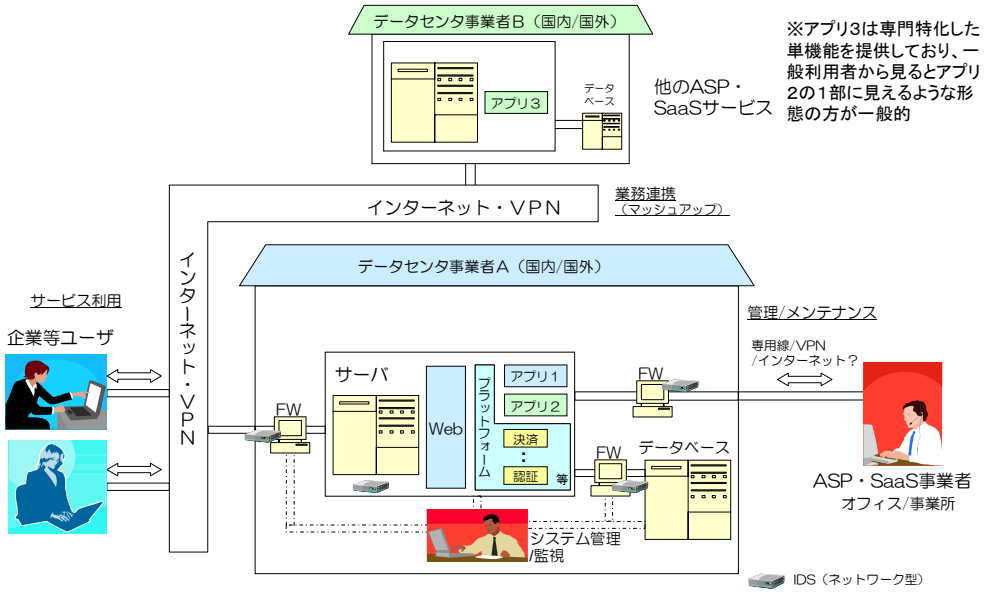
削除：を指す

＜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[23]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



削除：や

削除：、

削除：すること

削除：も

挿入：、Web ブラウザで

挿入：も可能である。

削除：である

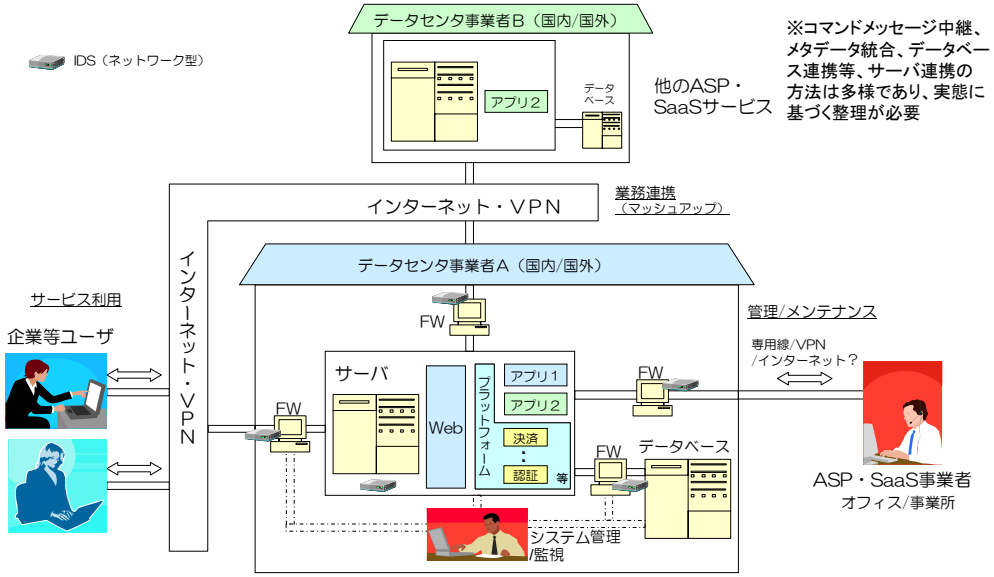
[23] Extensible Markup Language。データの意味や構造を記述することに使用されるコンピュータ言語の一つ。拡張性に優れ、コンピュータ同士でのデータの送受信やWeb ブラウザでの閲覧が可能。

＜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。

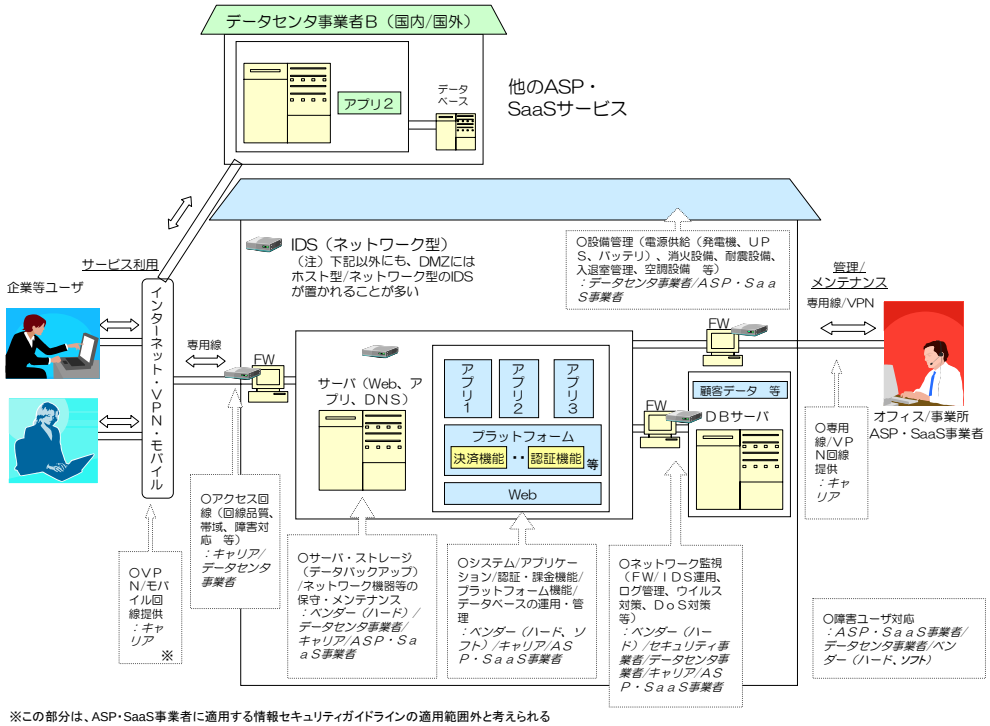
この形態の場合、メタデータ統合及びデータベース連携等、サーバ連携の方法は多様である。

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・ストレージ、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 における情報資産(表)**

分類	情報資産（構成要素＋情報）
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

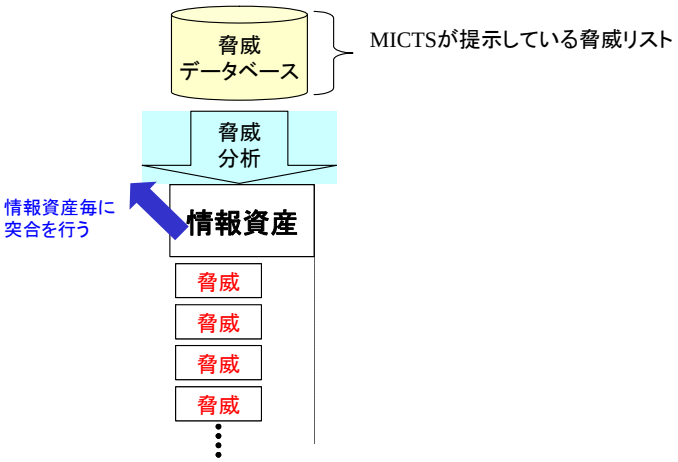
【4】 情報資産に対する脅威分析

【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

削除：ー

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

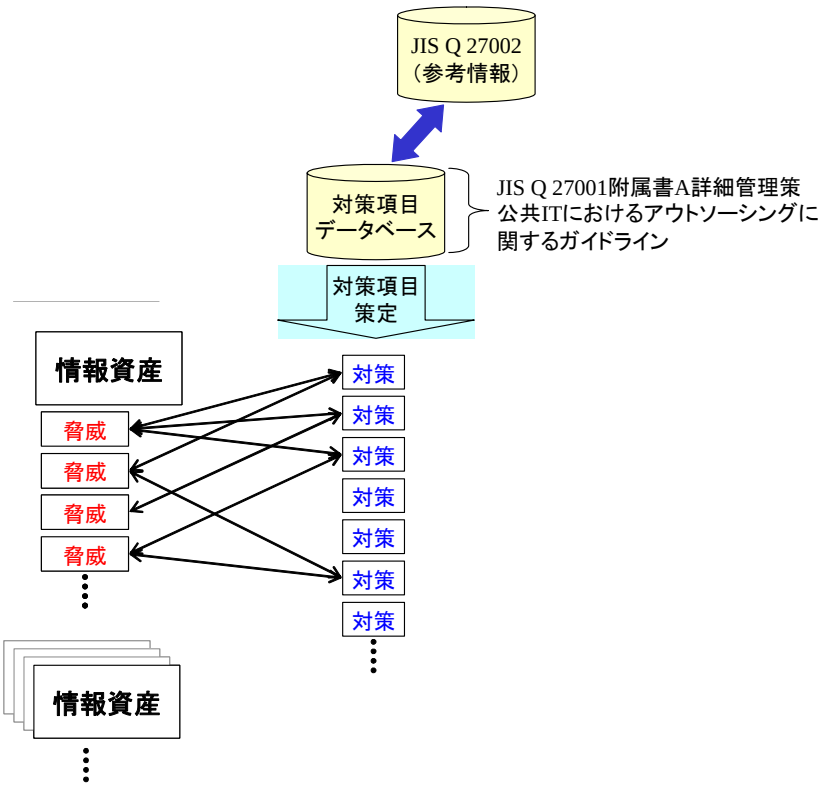
前項までの検討において、ASP・SaaS の構成要素から情報資産を特定し、各情報資産に対する脅威を抽出した。

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[24]。

[24] 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[25]や盗聴の対象になりやすい

(b) 対策導出の流れ

[25] インターネットなどのネットワークを使用して他のコンピュータに侵入し、改ざん・破壊、データの取得などの悪意ある攻撃を行うこと。

削除：を指す

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。

削除：。

(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】**

利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及び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（利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報等)、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

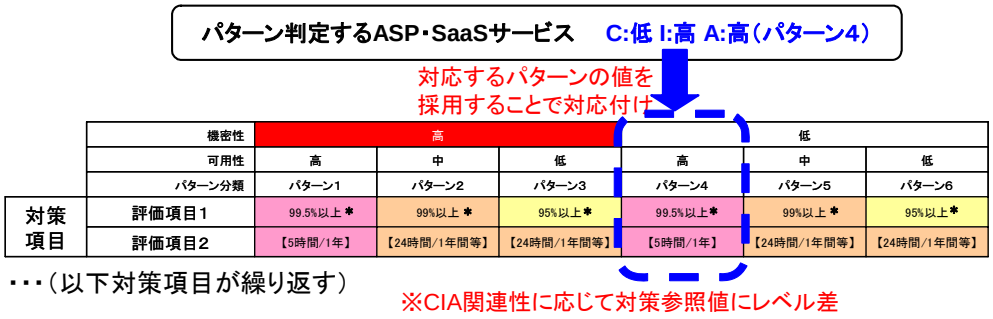
【1】項では、ASP・SaaS のサービス種別ごとに異なる CIA 要求に対応できるように、ASP・SaaS サービスを 6 つのパターンに分類した。本項では、当該パターン間で異なる CIA 要求を【5】項において導出した情報セキュリティ対策に対応付けし、多様な CIA 要求を持つ ASP・SaaS サービスに広く適用できる対策集を構築することを目的として、以下の手順により各対策項目に実施レベルを設定した。

- 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】

運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。 従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。 技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。

【評価項目】

a.　パターンファイルの更新間隔

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 3 日以内*
4	ベンダリリースから 24 時間以内*
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*

b.　OS、その他ソフトウェア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

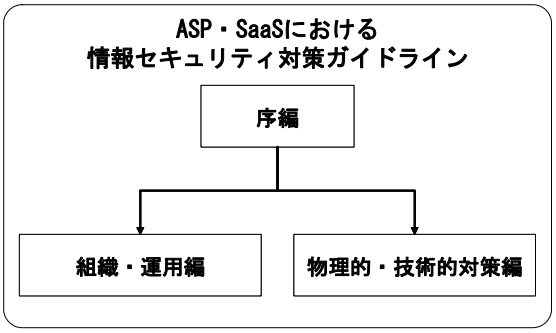
第一には、ASP・SaaS 事業者を想定している。

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遵守、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。

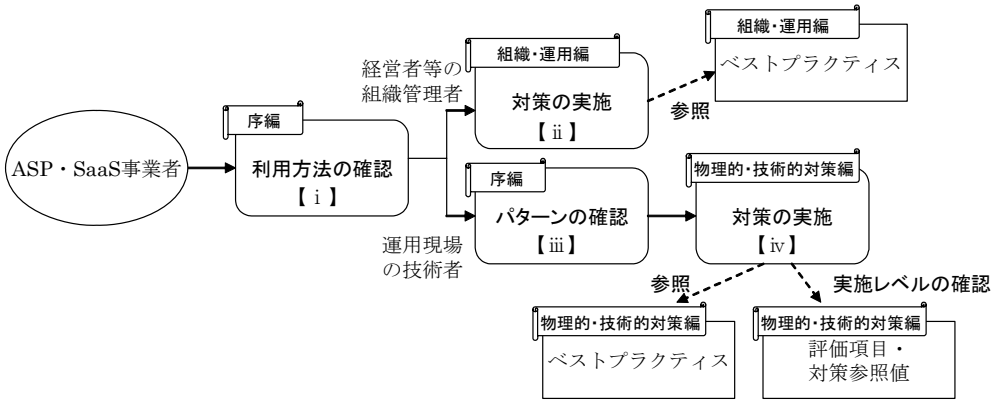
【２】運用現場における技術者等

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。

【2】ASP・SaaS サービス利用者における総合的な情報セキュリティレベルの向上

利用者にとっての二次的なメリットとして、ガイドラインに則って適切な情報セキュリティ対策が施された ASP・SaaS サービスの提供を受けることにより、利用者における総合的な情報セキュリティレベルの向上を図ることが期待できる。

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。

別　添

「ＡＳＰ・ＳａａＳにおける情報セキュリティ
対策ガイドライン」

（※添付省略）

参考資料Ⅰ（補足資料）

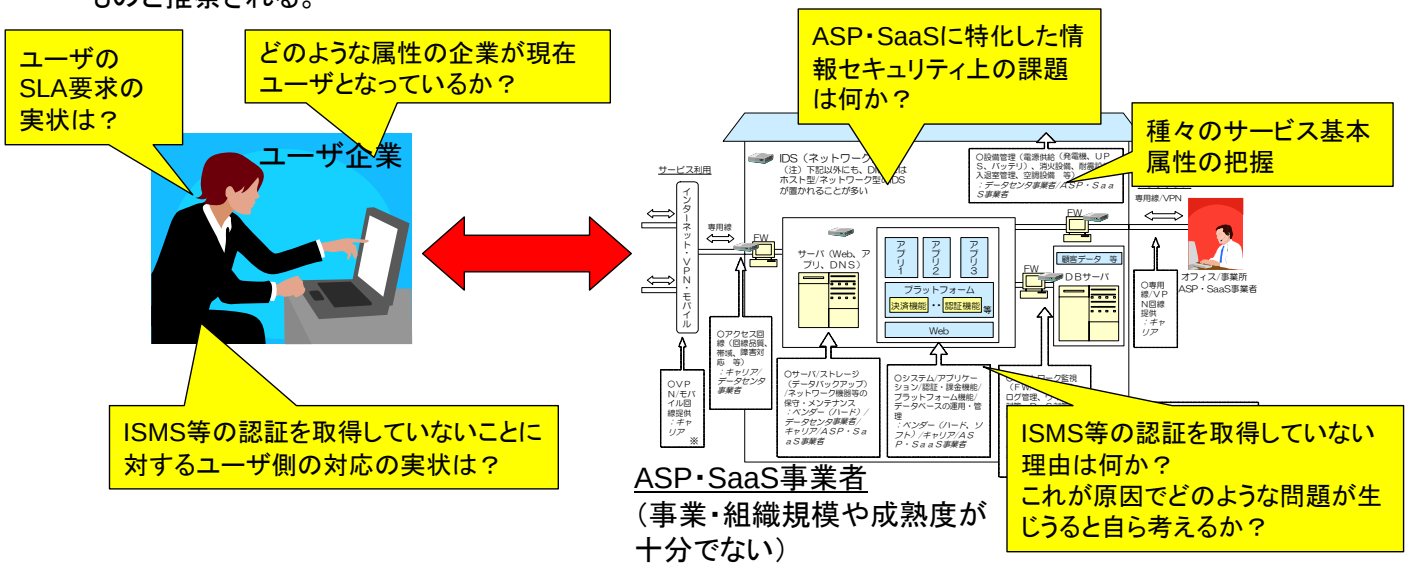
資料Ⅰ－1

ASP・SaaSにおける情報セキュリティ対策の動向 ①
～ASP・SaaS事業者へのインタビュー調査結果～

目次

調査の目的

ASP・SaaS事業者は、それぞれの規模に応じて、情報セキュリティ対策にいろいろと課題を抱えているものと推察される。



本調査では、事業規模とISMS/Pマークの取得状況をベースとして、認証を取得しづらい理由、認証を取得していない場合のASP・SaaS事業への影響、情報セキュリティ対策上の種々の課題等について実態を取りまとめた。

調査対象としたASP・SaaS事業者の概要

ASP・SaaS事業者9社に対してインタビュー調査を実施した。C社、G社、H社を除き、各社の売上規模は10億円未満である。ユーザーについても中小企業が中心である。

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 静脈・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

中小規模のASP・SaaS事業者のシステム構成及び運用の実状

中小規模のASP・SaaS事業者においても、データセンター利用が必要と考えているところが一般的である。また、サーバ/ストレージの運用は自社で実施しているところが多い（細かく実態把握したいため等の理由による）。さらに、他社との連携サービスについては、形態は種々だが、積極的に取り組まれている。

IDCの利用

売上規模	IDC利用	
	有	無
10億円以上	3社	0社
10億円未満	5社	1社

※IDCを利用していない会社は山形県にある自社の開発センターにサーバを設置

サーバ/ストレージの運用

売上規模	自社運用	IDCに委託
10億円以上	2社	1社
10億円未満	4社	2社

他社とのASP連携

売上規模	他社とデータ交換あり		Web画面表示上のみでの連携	他社との連携なし
	サーバ直結によるデータ連携	WebによるXMLデータ連携		
10億円以上	0社	1社	0社	2社
10億円未満	2社	1社	1社	2社（両社ともグループウェアサービスを提供）

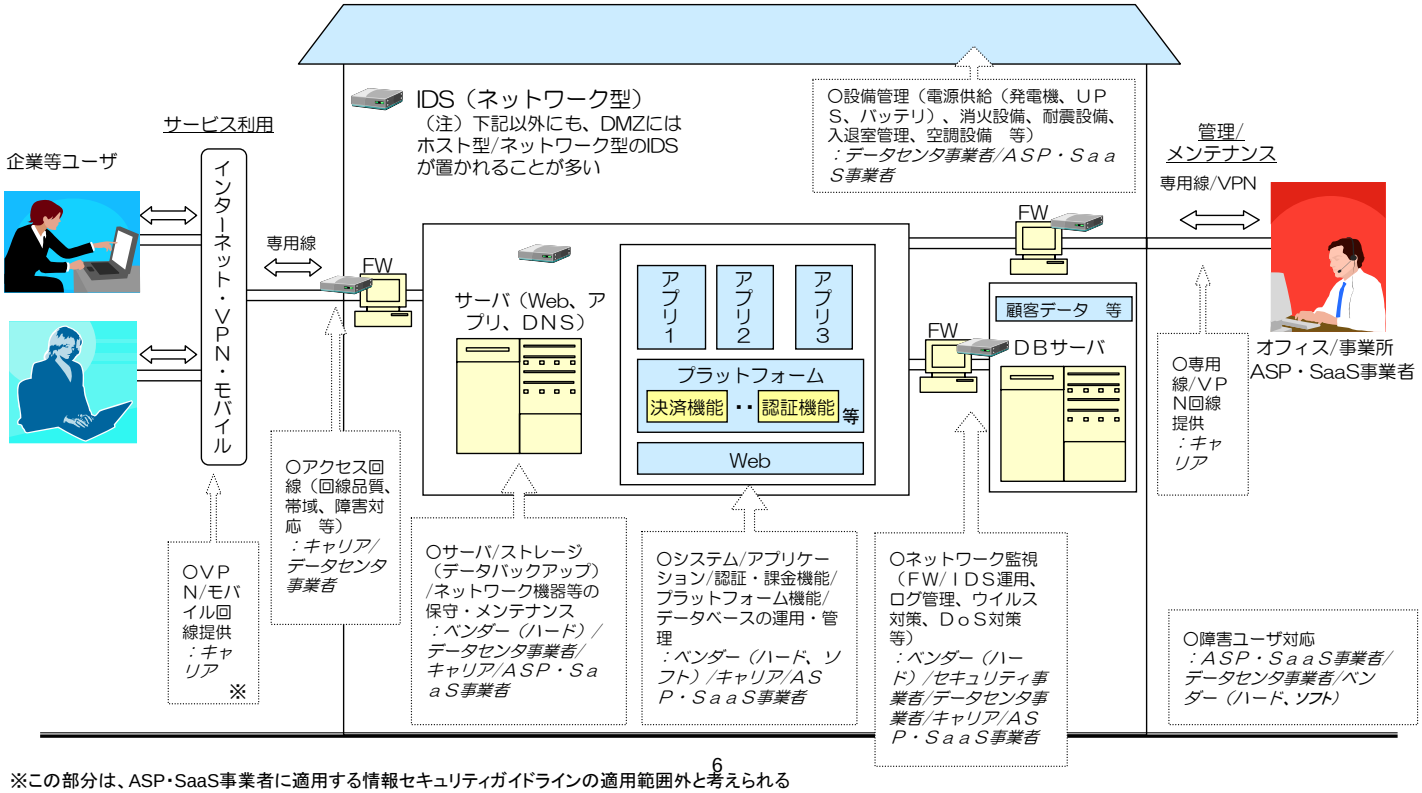
（参考）調査対象としたASP・SaaS事業者のシステムアーキテクチャと運用

調査対象としたASP・SaaS事業者のシステムアーキテクチャについて以下に整理した。

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

（参考）ASP・SaaSの典型的な構成要素

ASP・SaaSの4つの類型に基づくと、その典型的な構成要素は下図のように整理される。



※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

中小規模のASP・SaaS事業者の主たる情報セキュリティ対策の内容等

情報セキュリティに関する技術と運用は自社で確保している事業者が主流である。情報セキュリティ対策の実施メニューとしては大きな差はないが、取り組み姿勢、運用方法、SLA締結等について各社間に意識の違いがかなりあると見られる。また、大手であるH社を除いて、顧客からの厳しい情報セキュリティ要求にさらされていない様子を感じ取ることができる。

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。

ASP・SaaSに特化した情報セキュリティ上の課題について

各社とも、情報セキュリティに対する取り組み意識は決して低くないが、ASP・SaaSに特化した課題を抽出して重点的に対策に取り組んでいる実状はあまり見られない。その中で、以下のような課題を抽出することができた。

- 課題1： 情報セキュリティ対策における利用者と事業者の責任分界が重要である
  - 「ユーザ企業ID」と「ユーザID/パスワード」の組合せにより認証しているが、「ユーザID/パスワード」の管理をユーザ企業に委ねることにより、認証の責任分界点を設けている
  - 契約書において、システム障害や瑕疵に対する一般的な約款を設け、免責事項を明確にしている
  - フォレンジック技術を適用して、内部ログ管理を徹底し、またログの改竄や削除が容易にできない仕組みを組み込んでいる
  - ユーザーにセキュリティ運用に係る社内ガイドラインを設定していただいている
- 課題2： 事業者連携においては、エンドユーザと直接契約する事業者の情報セキュリティ規定が重要である
  - 帳票出力のような「縁の下の力持ち」的なサービスやIDC等のインフラ事業者は、エンドユーザに直接サービスを提供している事業者によるセキュリティレベル評価を受け、必要な情報を提供し、選択を受けることになる。従って、エンドユーザに直接サービスを提供する事業者の規定に沿う対応を行うことになる。
  - IDCのセキュリティレベルをどのように評価し、どのような基準で選択するかが課題である
- 課題3： 個人情報・機密情報に対する対策が重要
  - 中小事業者であっても、個人情報を扱っているという意識と、Pマーク取得への意欲が強い
- 課題4： ディザスタリカバリーについては、中小企業が多いASP・SaaSの場合、個別企業の努力でできることには限界がある
  - 別サイトにバックアップセンターの設置が可能なのは、相当収益が良い企業のみと考えられる

中小規模のASP・SaaS事業者のISMS/Pマーク認証の取得について

中小規模のASP・SaaS事業者は、個人情報を取り扱っているとの認識も高く、Pマーク取得には積極的であるが、ISMS取得には消極的である（特に売上規模が10億円未満の企業）。利用者から求められていない、取得コストが高すぎる等を主たる理由として挙げている。今後も、ISMS認証取得の必要性は認識しつつも、具体的な予定はないとしている。

ISMS取得

売上規模	ISMS認証取得		備考
	有	無	
10億円以上	2社	1社	―
10億円未満	0社	6社	・すべて具体的な取得予定なし ・3社は将来の必要性は感じており、そのうち1社は親会社グループの方針に従うとしている。

Pマーク取得

売上規模	Pマーク取得		備考
	有	無	
10億円以上	1社	2社	個人情報を取り扱わないため
10億円未満	3社	3社	・全社が個人情報を取り扱っているとの認識 ・取得している会社は、明確に取得の必要性を感じている

ISMSを取得していない理由

- 必要と感じていない、ユーザに与えるインパクトが疑問　等　⇒　利用者側から求められていないと推察される
- 取得コストが高すぎる
- 組織の成熟度も求められると認識している
- 親会社グループがグループ指針として「取得」を打ち出していない

（参考）調査対象としたASP・SaaS事業者の個人情報取扱及び認証取得の現状

中小規模の事業者であっても、個人情報を取り扱い、Pマークを取得している事業者が半数近くあった。Pマークが個人情報保護に特化した認証であり、対応範囲も絞りこまれることが理由と考えられる。これに対して、ISMS取得は、事業規模が大きい事業者でないと取得しづらいのが実態となっている。

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	情報セキュリティに係る認証取得状況		個人情報取扱の有無
			ISMS	Pマーク	
A社	財務会計システム	約5,000万円（2006年度）、5名	×	×	あり
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 静脈・指紋認証勤務管理	5.28億円 51名（国内）、100名超（海外含）	×	○	あり
C社	各種帳票出力サービス	70億円（2007.2）、203名	○	×（但し、個人情報保護方針をWeb公開している）	なし
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	×	○	あり
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）	×	○	あり
F社	物流･ロジスティクス効率化支援	5.2億円（2006.3）、15名	×	×	あり（1部顧客のみ）
G社	電車乗り換え案内、地図ASP	20億円、45名	×	×	なし
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	○	○	あり
I社	中小企業向けWeb会計システム	3.9億円（2006.3）、23名	×	×	あり

10

（参考）ISMSを取得していない理由と今後の取得意思について

ISMSを未だ取得していないASP・SaaS事業者は、将来も自発的には取得を考えていないところが多い。ISMS認証を取得していない理由としては、必要性の認識がないこと、コスト高、グループ企業のガバナンス方針等が指摘されている。

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	ISMS認証取得状況	ISMS認証を取得していない理由	ISMS取得に向けての意志
A社	財務会計システム	約5,000万円（2006年度）、5名	×	取得コストが高すぎる ユーザに与えるインパクトが疑問である	ユーザから要請があれば取り組みたい
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 静脈・指紋認証勤務管理	5.28億円 51名（国内）、100名超（海外含）	×	取得の必要性を感じていない （参考：Pマークは取得して当然と考えている）	取得予定はない
C社	各種帳票出力サービス	70億円（2007.2）、203名	○	－	－
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	×	親会社グループの方針が「取得」となっていないため（参考：Pマークは「取得」する方針） コストは問題ではない	親会社グループの方針に従う
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）	×	取得の必要性を感じていない （参考：Pマークは取得して当然と考えている）	取得予定はない
F社	物流･ロジスティクス効率化支援	5.2億円（2006.3）、15名	×	取得コストが重荷である 対顧客では、「自社管理の内容」と「IDCが取得している認証」によって理解を得ている。	将来は取得が必要と考えているが、現時点では具体化していない
G社	電車乗り換え案内、地図ASP	20億円、45名	×	取得の必要性を感じていない	取得予定はない
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	○	－	
I社	中小企業向けWeb会計システム	3.9億円（2006.3）、23名	×	取得の必要性を感じていない	将来は取得が必要と考えているが、現時点で具体化していない

11

ASP・SaaSにおける情報セキュリティ対策ガイドラインに対する要望・期待等 （1）

ASP・SaaSにおける情報セキュリティ対策ガイドラインに対して、次のような要望・期待等が寄せられた。

ユーザのASP・SaaS事業者選別の判断基準としての役割

ユーザ企業がASP・SaaSサービスを適切に選別できるようにするための判断基準になることが望ましい。

- 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
- ASP・SaaS事業者を単純に5段階等にグレード分けする指標を策定すれば良いのではないか。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「〇〇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
- ユーザにとっては、ASP・SaaS事業者が幾つ認証を取得しているかを確認する方が容易である
- 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。認定制度にすると、総務省が地元のITコーディネータと共に盛り上げようとしている地場に基づいたソフトウェア会社を潰してしまう可能性もある。
- ASP利用企業が安心して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

本ガイドラインの規模

本ガイドラインは、ASP・SaaS事業者の様々なサービス規模に対応できることが望ましい。

- 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
- ガイドラインのボリュームが大きくなると、市場の活性化が望めなくなる
- 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

ASP・SaaSにおける情報セキュリティ対策ガイドラインに対する要望・期待等 （2）

本ガイドラインの内容

本ガイドラインは、ISO等の標準的な規定に沿いつつ、情報漏えい等のリスクの影響判定を支援できるものであることが望ましい。また、新規参入事業者に対する指南書の役割を果たして欲しい。一方、技術やシステムに特化しすぎず、すぐに時代遅れにならないような内容とすることが望ましい。

- ガイドラインの内容は、ISO等の標準的な規定に沿ったものが好ましい。ガイドライン特有の特別な項目が策定されると、標準的な規定に加えて、これらにも対応しなければならなくなる。
- ASP・SaaSサービスの使用用途に応じた情報漏えいの影響の有無はどう判定するのかという問題がある
- 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
- テクノロジーやシステムに特化すると、ガイドラインが策定できた頃には時代遅れとなってしまう可能性がある

本ガイドラインの運用

本ガイドラインは、業界の自主的な取り組みを尊重する中で、継続的に遵守されることが望ましい。自己申告制のようなコミュニティベースの仕組みによる運用も考えられる。

- ガイドラインを策定するならば、毎年その遵守に対する監査を行うなどで継続的に遵守しなければならないと思われる
- 国の投資でサイトを立ち上げ、自己申告制でチェックリストを作成・公開するような仕組みが考えられる。また、ID認証された事業者のみがコミュニティベースでグレードを分け、これを公開するような仕組みを取れば、低コストで運用できるため現実的ではないか。
- ガイドラインは強制的な認証制度ではなく、業界の自主ルールとする

資料Ⅰ－2

ASP・SaaSにおける情報セキュリティ対策の動向②
～ASP・SaaS事業者における取り組み事例の紹介～

目次

ASP・SaaSの情報セキュリティ対策に関する研究会

ASP・SaaSの動向
と
セキュリティに関連する課題

2007年 6月21日

特定非営利活動法人 ASPインダストリ・コンソーシアム・ジャパン

V1.0

内　　容

- ASP・SaaSとは
- ASP・SaaSの市場規模推移
- ASP・SaaSにおけるセキュリティ関連の課題
- 求められる対応
- 参考資料

ASP・SaaSとは・・・定義

定　　義

特定及び不特定ユーザが必要とするシステム機能を、ネットワークを通じて提供するサービス、あるいはそうしたサービスを提供するビジネスモデルのこと

留意点：ASPと類似の用語として「ユーティリティコンピューティング」「オンデマンドコンピューティング」「SaaS（Software as a Service）」などが存在するが、ほとんどASPと同一の意味で使用されている。

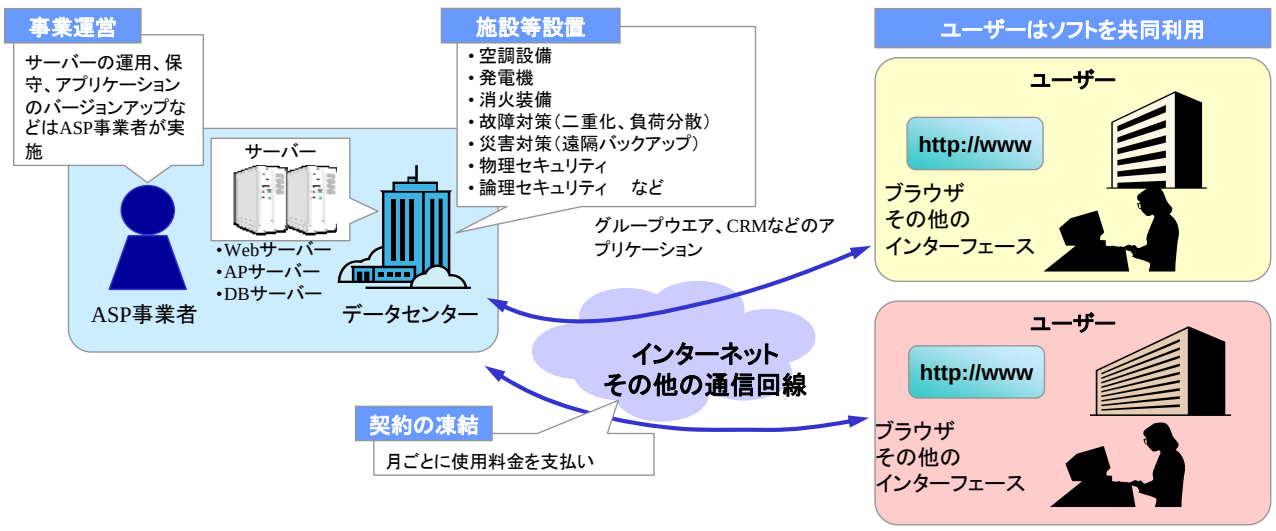
（カスタマイズ性やAPI公開などの特性で分類する動きがあったが、すでに

混在化して区別はできない状況にある）

出所：「ASP・SaaSの普及促進策に関する調査研究」
（H19年4月、総務省、ASPICジャパン）

ASP・SaaSとは・・・システム形態

ASP・SaaSのシステム形態



ユーザーが必要とするシステム機能を，ネットワークを通じて提供する。ユーザーはブラウザを通じて利用し，使用料金を期間（毎月払い、一括払いなど）に応じて支払う

ASP・SaaSとは・・・従来から見た最近の傾向

	ASPとのみ呼ばれていた時代（1998～2004頃）	ASP・SaaSの時代（2005頃～）
ASP/SaaSを前提として設計	×	○
操作性	応答性悪く、操作性今一つ	Ajaxの採用などにより向上
サーバーの共有化形態	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
サーバーごとのソフトウェアコードの同一化	×（部分的には異なる）	○（記述言語など統一可能）
ユーザー側でカスタマイズする際の作業性	×	○（メタデータの採用等）
他のアプリケーションとの連携	×	○（連携用APIを公開等）

出所：日経BP Webページ　http://itpro.nikkeibp.co.jp/article/lecture/20070219/262353/
よりASPICジャパン分析

ASP・SaaSとは・・・基本的ユーザーメリット

ICT化を進めるユーザーが抱える課題・問題		左記の解決に役立つASP・SaaSのユーザーメリット
1．コスト	● ICTの利用用途や枠組みが増大 ● ICTコストの絶対値も増大	● 無駄なハード、ソフト、SE人件費を削減－－主要部分の集中化、共同利用による
2．リテラシー対応	● さらに高度なIT技術が今後とも増大 ● ノウハウ維持の手間が増大 特に中小企業で困難化	● 専門事業者による高いレベルのノウハウで運用
3．セキュリティ対応	● セキュリティを自分で守ることが困難化	● IDCやセキュリティシステムなどによる、災害・停電・ネットセキュリティ・人的管理に対応する環境での運用
4．新しいビジネスモデルによる付加価値拡大	● サービスの付加価値向上が重要経営課題に	● より便利で有効な利用環境の付加－－情報共有・有機的活用 ● 新しいビジネスモデル創出（商品・サービス・コンテンツの流通

これらは特に中小企業で有効となる性質をもつ

ASP・SaaSとは・・・中小企業にとっての競争力

経営改善：経費改善（間接費）

守り

競争力強化
・高度な効率化経営
・魅力度アップ
・新しい付加価値獲得

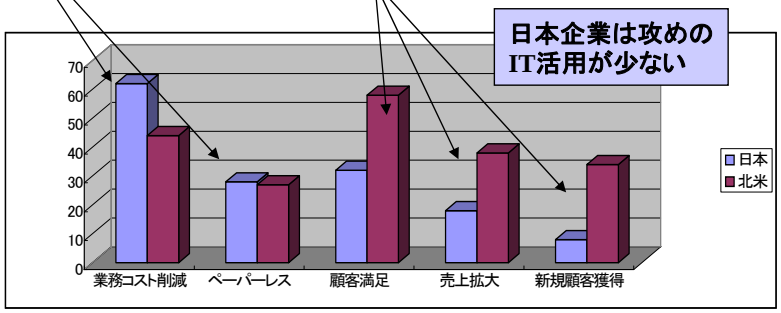
1．IT投資部分の複雑化と増大
→ITも大きな経営上のコスト・IT人材不足
2．よりITに依存した経営・業務・仕組み
→ITトラブル・ウイルス＝経営危機に直結
3．中小企業も国際的な効率・戦力確保の競争
→グローバル・メタナショナル経営
4．コンプライアンス・企業責任
→個人情報漏洩などへの対応

守りを必要とする経営環境

ASP・SAAS
→IT環境の効率化
→より高度なIT活用

ビジネスイノベーション

攻め



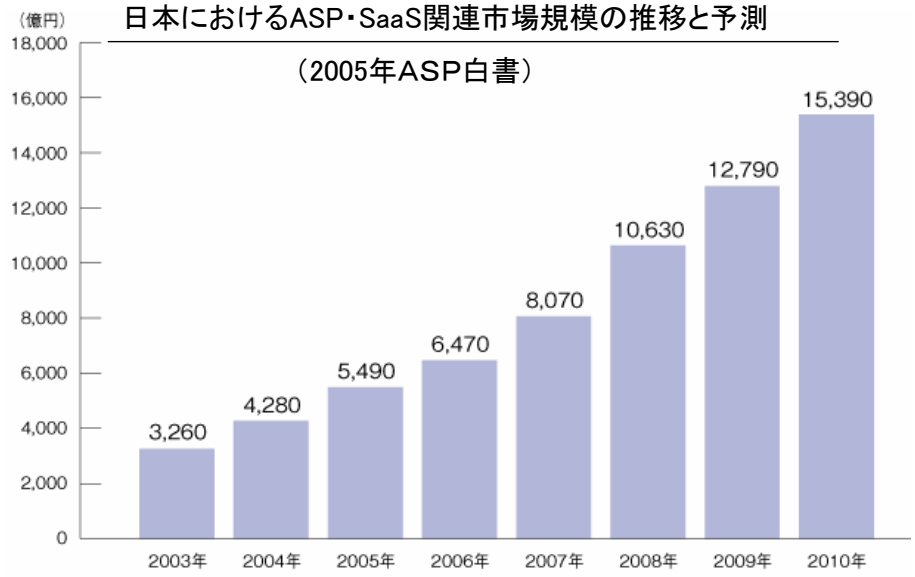
出展：ガートナージャパン（07.03.09.日経産業新聞）

攻めを必要とする経営環境

1．新しいマーケッティング
→顧客確保・顧客嗜好の把握
（ネット活用・ASP連携が競争の重要要素）
2．より高度で複雑な時代への対応
→企業に求められるナレッジベース
・情報共有・インテリジェンスパワー
・コミュニケーションパワー

出展：ASPIC津田常務理事講演資料

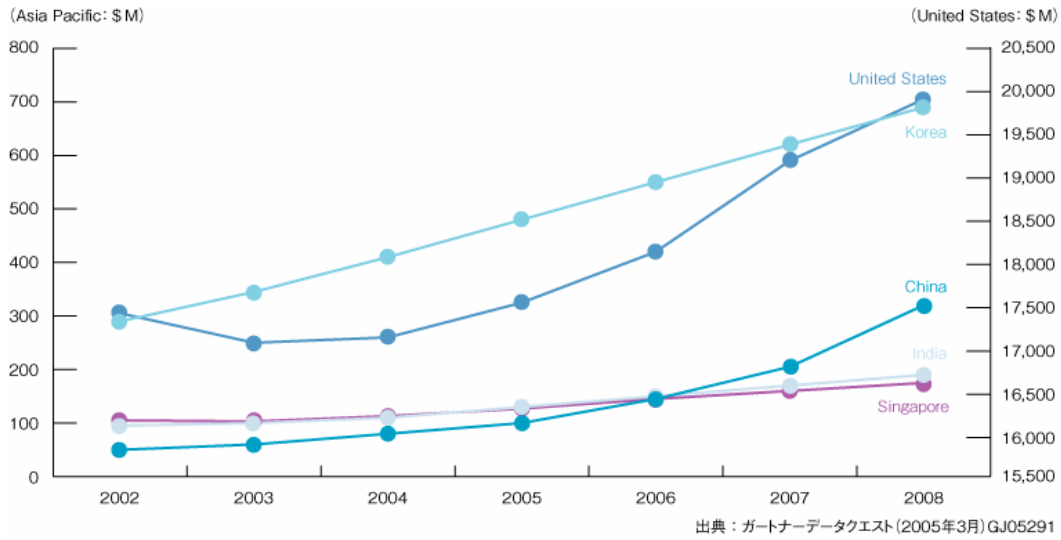
ASP・SaaSの市場規模推移（1/2）



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。

ASP・SaaSの市場規模推移(2/2)

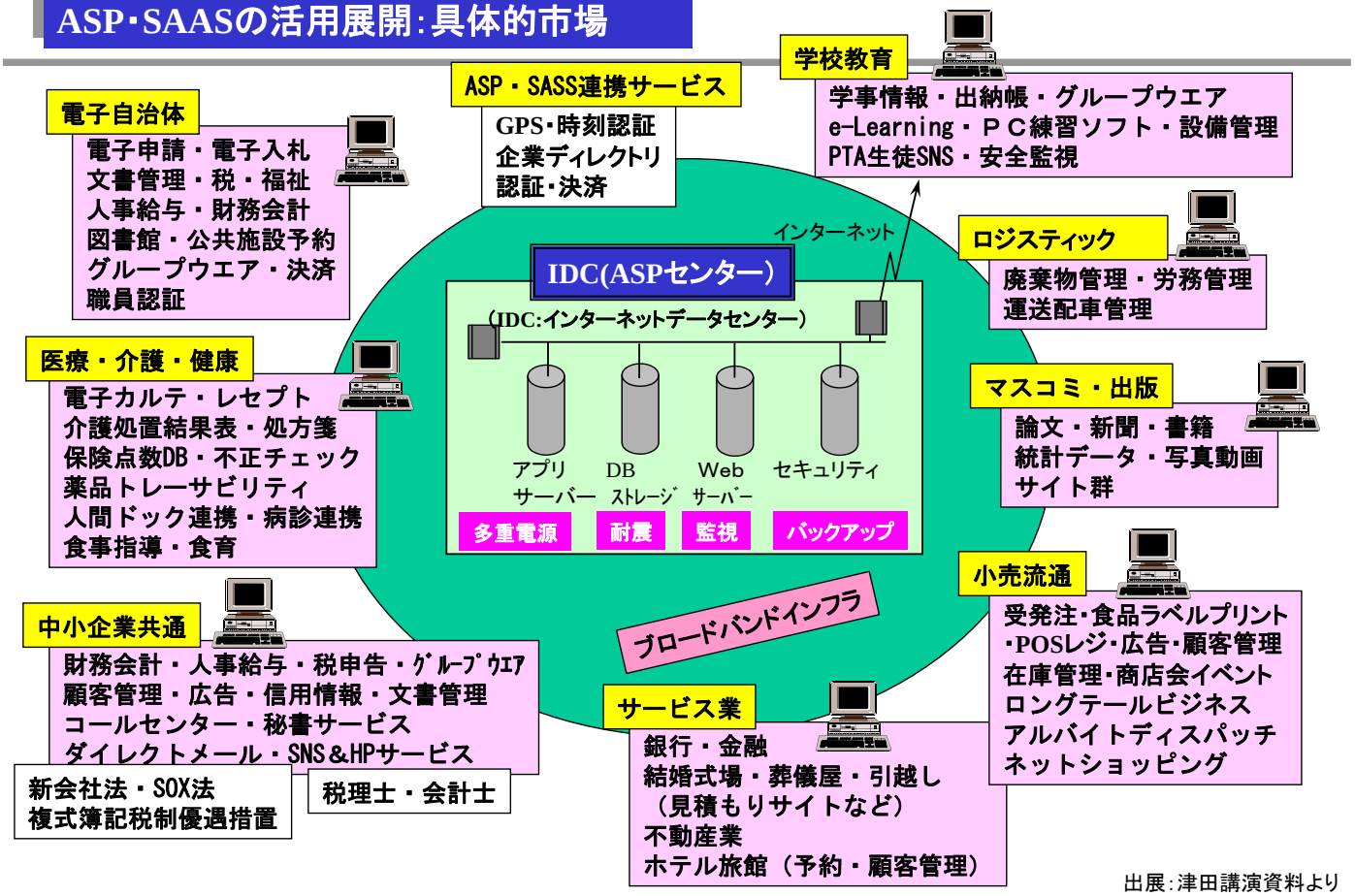
各国のASP・SaaS市場規模の推移と予測



米国では2008年で約2兆円

2005年ASP白書

ASP・SAASの活用展開:具体的市場



出展:津田講演資料より

ASP・SaaSのセキュリティに関連する課題

ASP・SaaSの進展・市場拡大

⇕

セキュリティ・安全性？？？？

- ASP・SAASの提供事業者は、中小ベンダーも多い
  →充分な情報セキュリティ対策が施され　ていない可能性が高い（EX.雑居ビルで　のサーバー運用）
- 顧客へのセキュリティ関連情報公開
  →充分ではない。セキュリティのレベルが　どの程度か不明な場合が多い
  →ユーザーは、サービスの選択基準が不明で、不安も残る
- これらが改善されると
  →さらにASP・SaaS市場が拡大する可能性がある。

中小企業のIT化課題の一つ：セキュリティ

⇕

セキュリティ対応は中小企業には難しい（投資・ノウハウ）

- 経済財政諮問会議でも、IT化が米国に比較して優位ではないことが指摘されており、情報セキュリティ対応にも問題が潜在していることが推定される。
- このような中、情報システムを自社開発していく余裕のない中小企業にとって、ASP・SAASの利用は、IT化を推進する原動力となるものである。
- 一方で、適切な情報セキュリティ対策の施されたASP・SAASを利用することで、ユーザーにとってのセキュリティが向上していく効果が見込まれることとなる

ASP・SAASの良い部分がより多く享受されるように、情報セキュリティに関する実態等を把握し、提供事業者が講ずべき情報セキュリティ対策と顧客への提示方法を整理することが必要

求められる対応の方向

対応策1

ASP・SAASにおける現行のセキュリティ対策レベルを踏まえ、どのような構造・どのような事項がセキュリティの向上に貢献するのか分析・整理、特にASP・SAASならではのセキュリティに配慮すべき点はなにかを整理する。

対応策2

現状のセキュリティ関連の認証・ルール・しくみが、ASP・SaaSの展開に、合致しているのか、不足な点はなにかを調査整理する。

対応策3

整理され、顧客が理解しやすいような、ベンダー側から顧客に提示する項目や数値の単位などのガイドを策定（→カタログ・契約書・約款などに反映を促す）

EX. 表示必須項目と付加項目

EX. 比較可能な数値単位とサンプル数値

EX. 国外のデータセンターを活用する場合に顧客に知らせるべきか？必要ないか？

EX. 問題発生後のPDCAサイクルの問題解決（CMUでの評価制度）

EX. 一般的な認証の表示（Pマーク・ISO）

・・・・・その他

把握すべき事項

①ASP・SaaSはユーザのセキュリティ向上をどのような仕組みで果たすことが出来るのか？

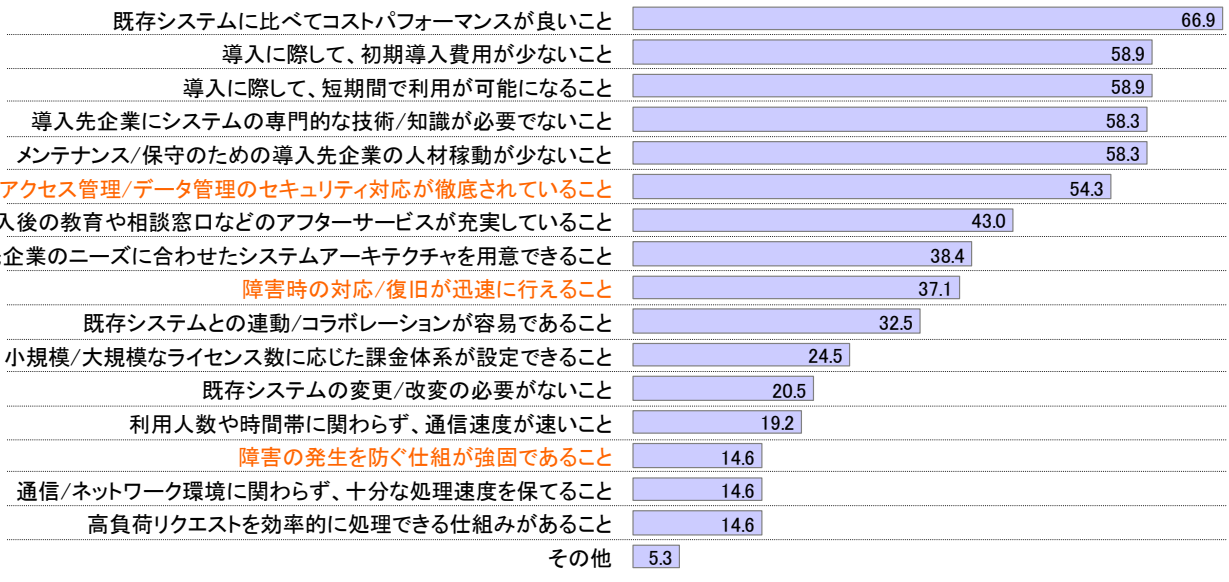
②現在用いられているガイドライン、基準にはどのようなものがあるか？

参考資料

ASP・SaaSの顧客からの期待

サービス提供事業者が想定している顧客からの期待
〔複数回答〕

N=151（単位：%）



ASP・SaaSのシステム構成

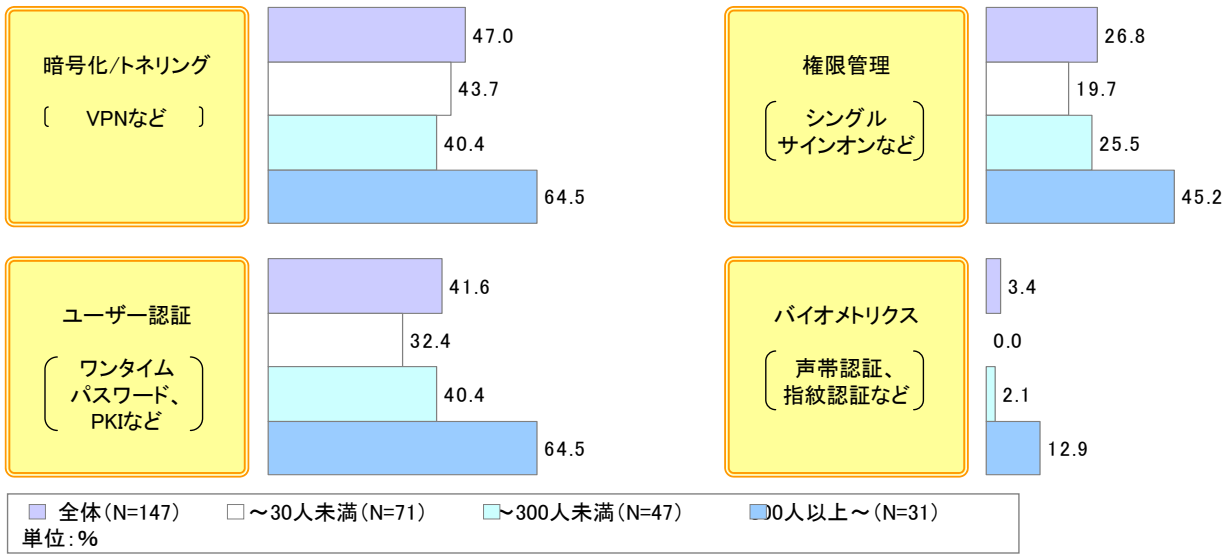
ASP・SaaSのシステム体系

システム分類名称		具体例					
業種別／分野別 ASPアプリケーションサービス		一般向け フロントオフィス業務（営業支援等） バックオフィス業務（給与、人事、会計、総務、財務、等）	製造業向け	流通業向け	建設業向け	公共向け	…
共通 ASPサービス	共通アプリケーション	グループウェア(情報共有、メール配信等)	TV会議／Web会議	…			
	アプリケーション基盤	認証基盤	文書管理基盤	決済基盤			
	システム基盤	ネットワーク監視	不正アクセス監視（IDS）	ウイルスチェック	…		
ASP型 ネットワーク基盤サービス		VPNサービス	外部／イントラネット接続サービス	コールセンターサービス	…		
システムインフラ		IDC(インターネット・データセンター)	通信ネットワーク	…			

ASP・SaaSのセキュリティ対応状況（1/3）

➢事業者のセキュリティに関する対応状況を以下の4視点でみると、「暗号化/トネリング」「ユーザー認証」は比較的浸透しているといえるが、未対応の事業者も半数以上と多い。「権限管理」に関しては、大規模の事業者においてのみ、ある程度浸透しているといえる

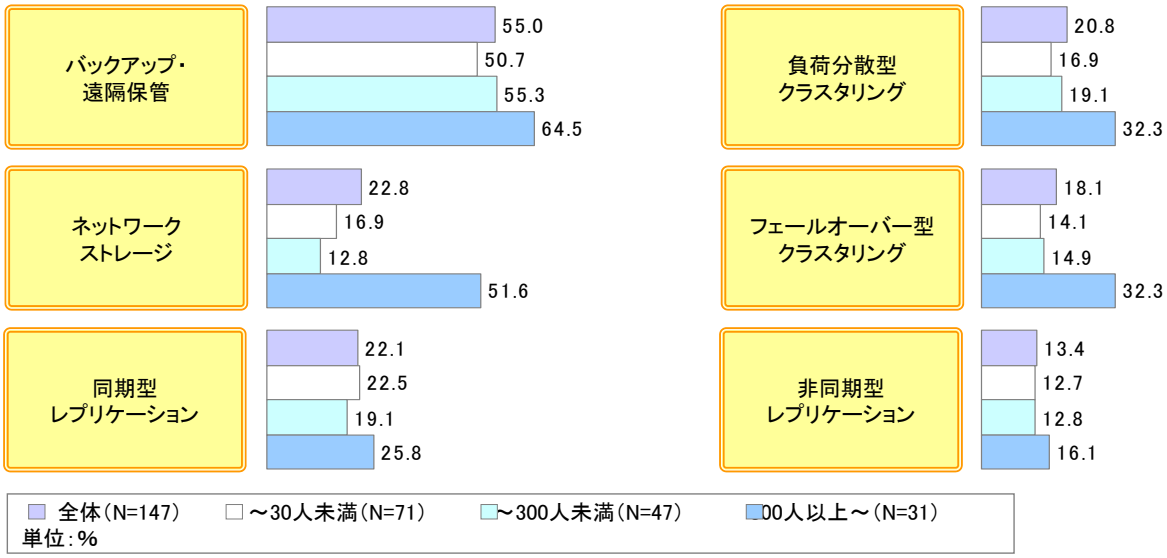
ASP事業者の対応技術（事業者の従業員規模別）
〔セキュリティについて〕



ASP・SaaSのセキュリティ対応状況（2/3）

➢事業者の障害対策に関する対応状況を以下の6視点でみると、「バックアップ・遠隔保管」は規模の大小に関わらず浸透しているといえる。他の障害対策はあまり浸透していないが、SANやNASといった「ネットワークストレージ」は大規模の事業者においてのみ浸透が進んでいる

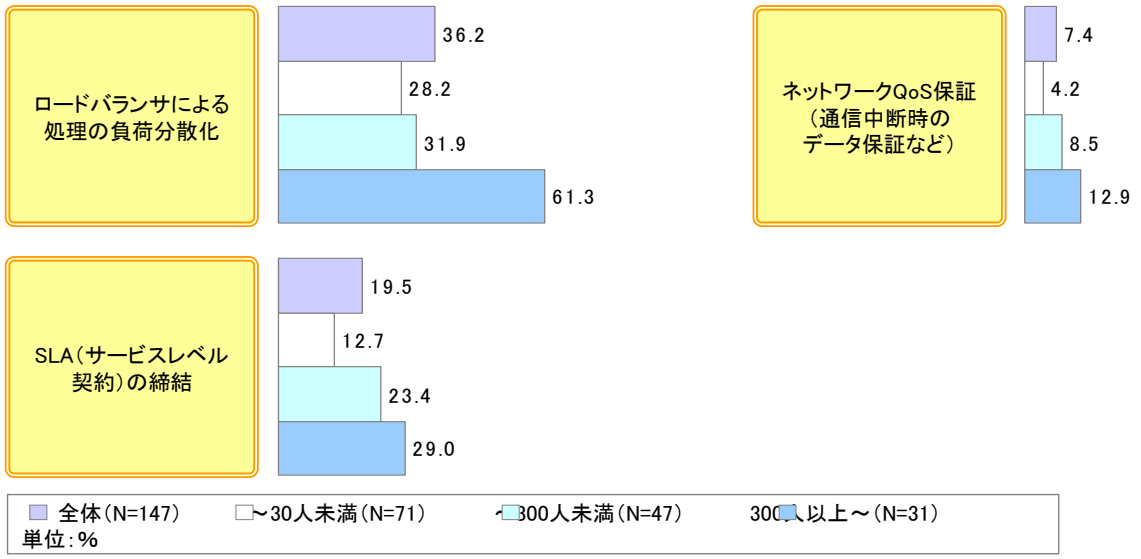
ASP事業者の対応技術（事業者の従業員規模別）
〔障害対策について〕



ASP・SaaSのセキュリティ対応状況（3/3）

➢事業者の品質保証に関する対応状況を以下の3視点でみると、大規模の事業者においてのみ「ロードバランサによる負荷分散」が浸透しているといえる。「SLA」や「QoS」などのサービス保証は、規模の大小に関わらず、未対応の事業者が非常に多いといえる

ASP事業者の対応技術（事業者の従業員規模別）
〔品質保証について〕



（第1回研究会　資料1－5）

株式会社富士通ビジネスシステム
FUJITSU BUSINESS SYSTEMS LTD.

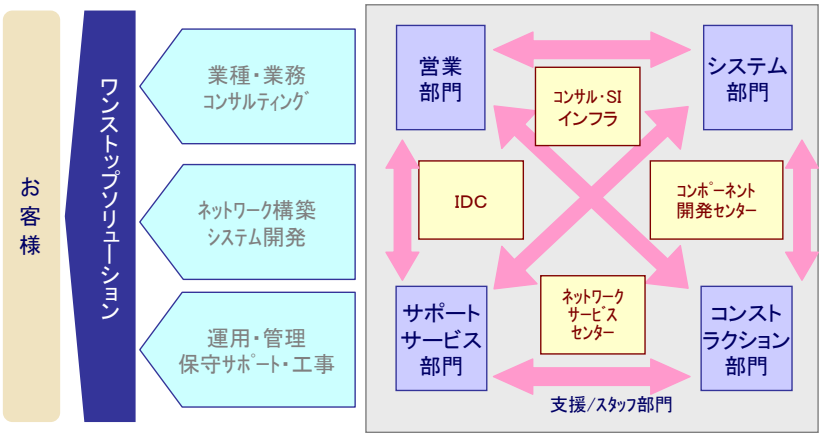
ASPビジネスの状況について

株式会社富士通ビジネスシステム
システム本部アウトソーシングサービス統括部
ITアウトソーシングサービス部
今田　正実

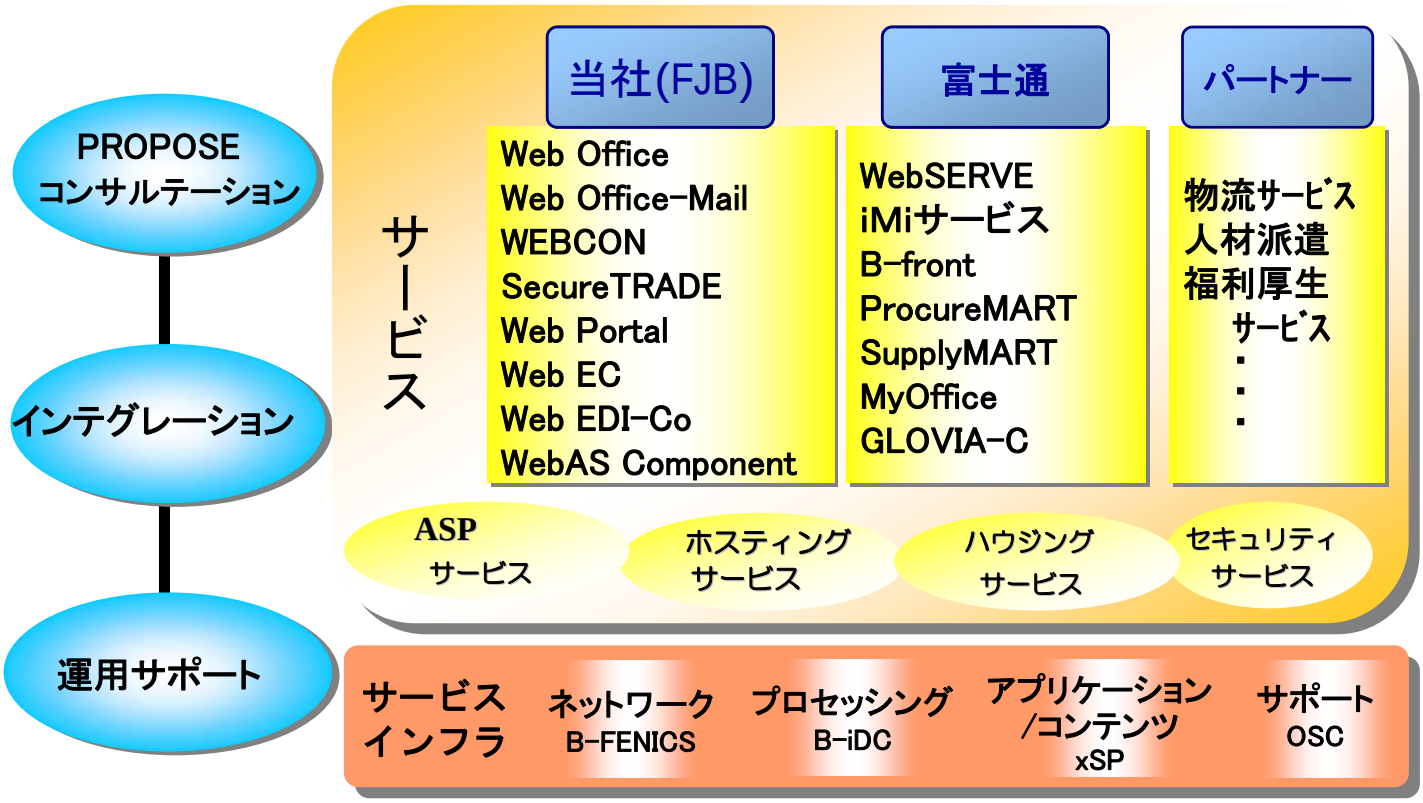
1．会社概要

- ■社名 株式会社富士通ビジネスシステム　FUJITSU BUSINESS SYSTEMS LTD.
- ■所在地　本社：〒112-8572 東京都文京区後楽 1-7-27　営業拠点：28ヶ所、サービス拠点：107ヶ所
- ■設立　昭和22年4月23日　■資本金　122億 2,000万円　■株式　東京証券取引所 市場第一部
- ■事業内容　通信と情報のシステムインテグレータ企業として、コンサルティングから、機器販売、ソフトウェア開発
- 設置工事、保守までの一貫したサービスの提供
- ■従業員数　単独：3,239名、連結：3,345名　（2006年9月末現在）
- ■売上高（連結決算）　平成17年度：162,486百万円、平成18年度中間期：71,615百万円

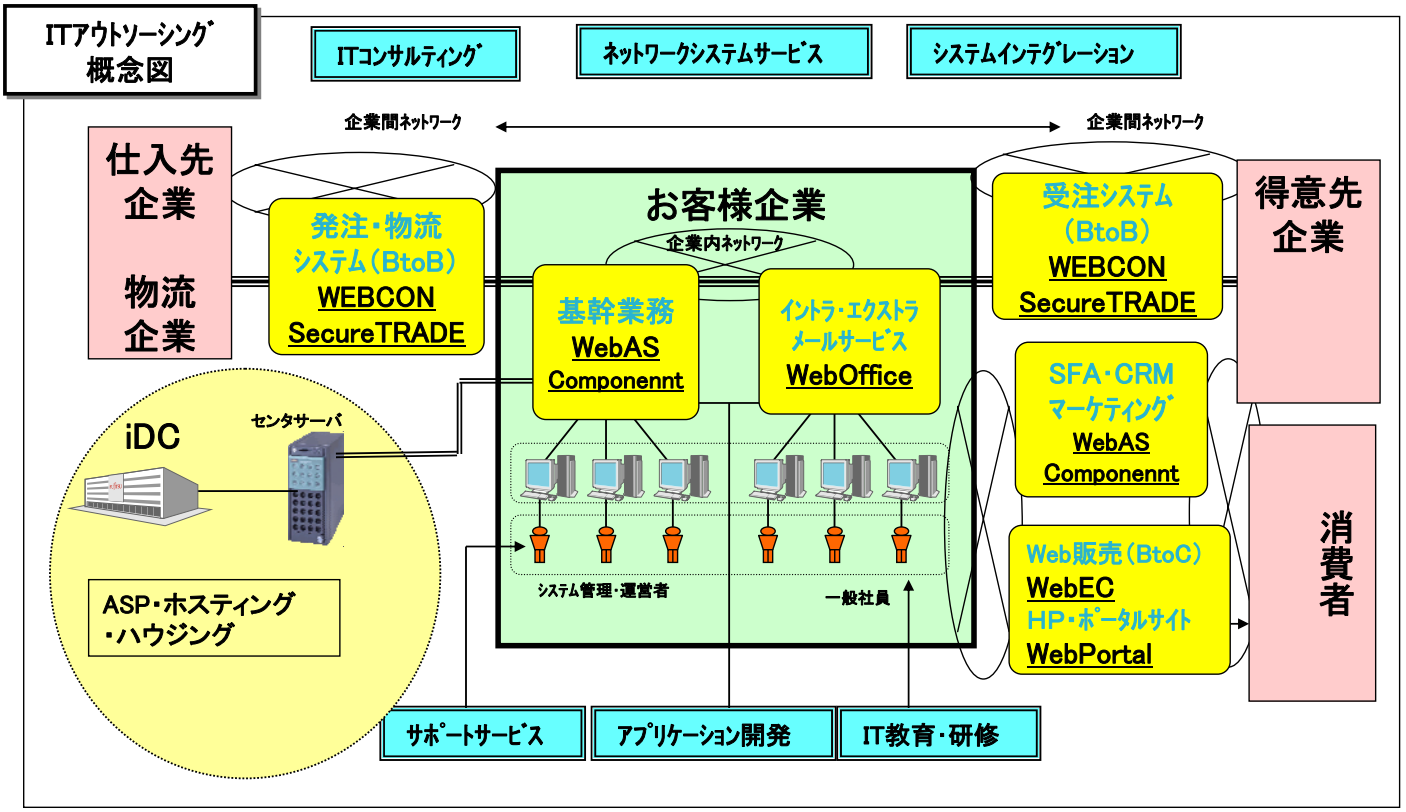
当社の特徴
■ ワンストップソリューション〔営業、SE、CE、コンストラクション〕
■ 全国サポート〔営業拠点28ヶ所、サービス拠点107ヶ所〕
■ カスタマーベース 約4万社のユーザ 〔全業種対応〕



2. アウトソーシングソリューション体系



3. ITアウトソーシング全体概要



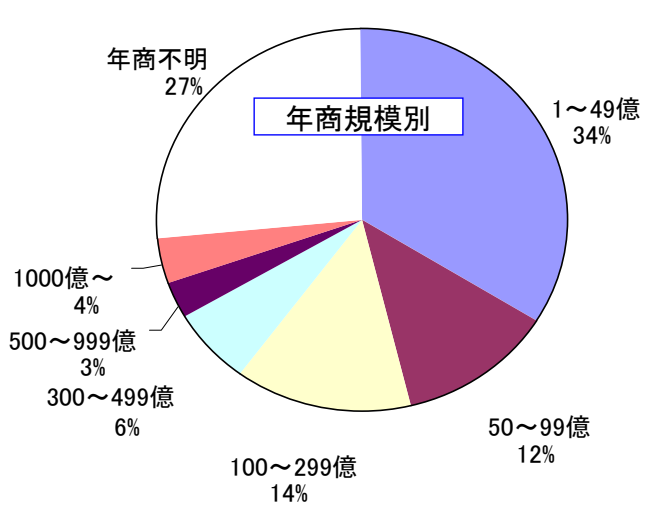
4. WebOffice（ASPサービス）概要

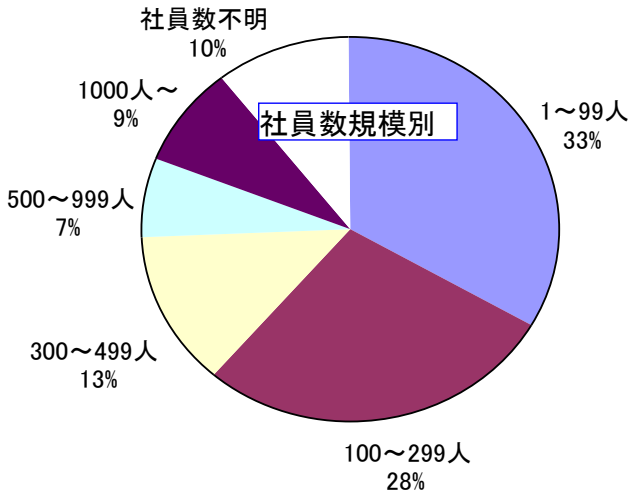
- インターネット創設期（1997年）よりのASP型での老舗グループウェアサービス。
- 長い実績から得たノウハウとお客様からの多数のご要望から生まれた使いやすく便利な機能を
- 定期的に反映する無償バージョンアップを実施しています。お客様の自由度を上げる機能として
- トップ画面の画像変更やレイアウト変更も可能な上、自由なフォーム画面作成によるアンケート
- 集計やワークフローも利用できます。また、内部統制やコンプライアンスを重視した機能として
- 掲示板発言ログ確認機能や各種履歴管理ができます。

5. WebOffice年商/社員数規模別導入企業状況

WebOffice導入企業状況

不明の数値には病院・学校・自治体などが含まれています。

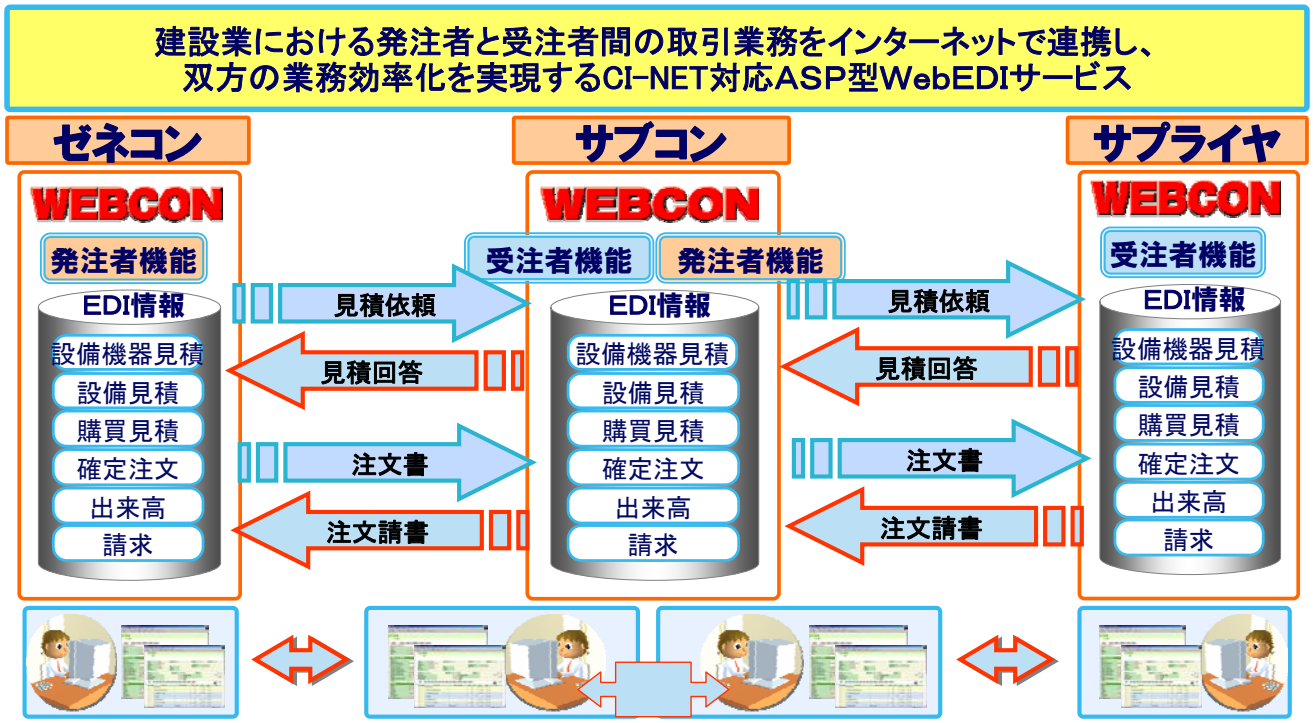




年商300億円以下が60%、社員数300人未満も61%
中小企業の利用者が多い。

6. WEBCON（ASPサービス）概要

CI-NETに準拠した建設業向けWebEDI（ASPサービス）として、2003年よりサービス提供。



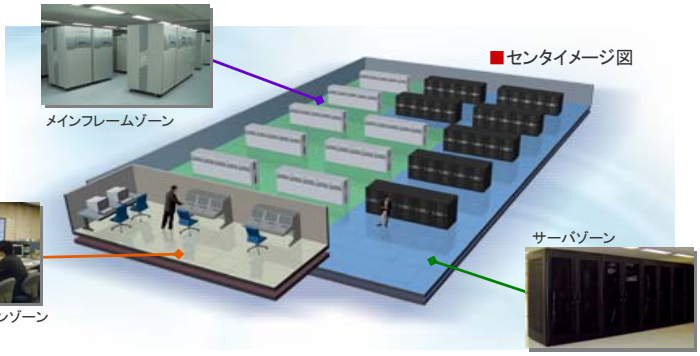
8. セキュリティへの対応

- 企業として、ネットワーク社会の健全な発展を希求し、また、情報・通信システムのソリューション
- をお客様に提供・サービスする企業の責務として、情報セキュリティの強化を、最も重要な経営
- 課題の一つとして捉えています。
- これまでも、02年に「FJB 情報セキュリティポリシー」を策定したのをはじめ、対外資格の
- 「プライバシーマーク」や「ISMS」等の取得にも努め、さまざまな努力を積み重ねてきました。
-
- センター管理としてはハイレベルな安全対策を施したファシリティ、ビデオカメラによる監視システム
- 防犯センサー、二重チェック入退室管理システム、マシン室への入室には指紋認証実施など最先端の
- 機能により対応しております。
-
- 尚、セキュリティ面では、富士通グループの厳格なセキュリティ対策基準に認定済みであり、
- 定期監査を継続的に実施し、問題があれば随時是正しています。
- ※データセンタでの監視サービスは、2006/9月、ISO27001認定取得済み
- ネットワークサービスセンターが提供する監視サービスは、2007/3月、ISO20000認定取得済み


自家発電装置
(GTG)


監視カメラ


専用カードによる
入退室



Best Solution & Best Partner

今日、そして明日のベストを求めて
FJBは、常に核心をつくソリューションを提供し
お客様の経営・事業の良きパートナーを目指します

（第1回研究会　資料1－7）

SaaSがもたらす新しい世界
On-Demand Platform for the Business Web

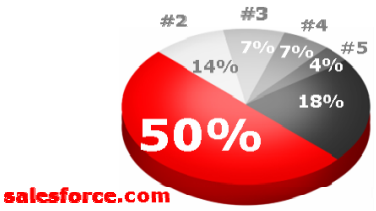
株式会社セールスフォース・ドットコム
チーフテクノロジーオフィサー

及川喜之

salesforce.com
Success On Demand.℠

セールスフォース・ドットコム 会社概要

- 99年創業、2000年4月サービス開始、2004年6月NYSE上場
- 2007年度売上額 USD 497.1M（対前年比60%増）
- 本社：サンフランシスコ
- サービス提供形態：Software as a Service (SaaS)
- オンデマンド市場においてNo.1のシェア （2006年9月実施のIDC調査報告による）
- 会社創業時より社会貢献活動に取り組む
- 数多くのアワードを受賞



あらゆる業種・業態・規模にわたる導入実績

Innovation. Not Infrastructure.

サービス
THE WESTIN OSAKA
ANA Learning

ITサービス
GDO GOLF DIGEST ONLINE
CyberAgent
VALUECOMMERCE
IPLOCKS

金融
FXCM
損保ジャパンDC証券
KBC
MIZUHO

ハイテク・ソフトウェア
Canon
RICOH
FUJITSU 富士通ミドルウェア
ELECOM

製造業
YAMAHA
日清製粉グループ
日清フーズ株式会社
Nitta Gelatin Inc.

メディア・通信
SoftBank
KDDI 株式会社
Panasonic
@nifty

SIer
NS Solutions
iSiD
コベルコシステム株式会社
HitachiSoft

流通・小売
Johnson&Johnson
sanyoichi.com
NEXUS

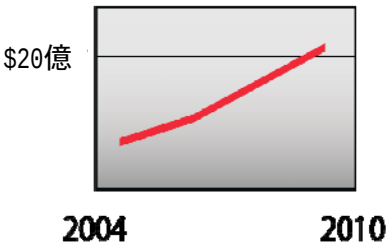
不動産・建設
流体計画
ライフステージ
株式会社 セイクレスト
IZUMIGO

The End of Software（ソフトウェアの終焉）

予想以上の速さで「オンデマンドの時代」に移行しつつある

31%成長

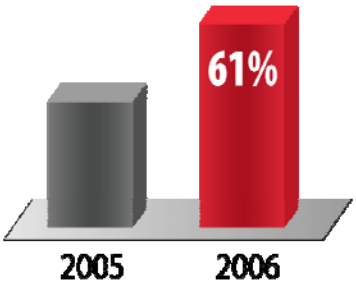
オンデマンドCRMの
年平均成長率



IDC

61% 成長

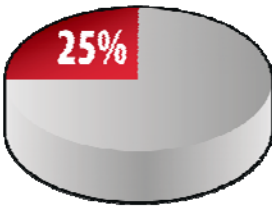
企業における採用



McKinsey&Company

25-40% 普及率

2,200億ドル規模の
ソフトウェア産業



Gartner

ミッション: On-Demand Platform for the Business Web

メインフレーム

IBM

digital

クライアントサーバー

ORACLE
SIEBEL
PeopleSoft
SAP
Microsoft

オンデマンド

Google
ebay
amazon.com
salesforce.com

マルチ・テナント方式の必要性

The Business Web™（ビジネス・ウェブ）を実現するマルチ・テナント方式
一般消費者向け Web と全く同じ

SAP　Microsoft　ORACLE

vs.

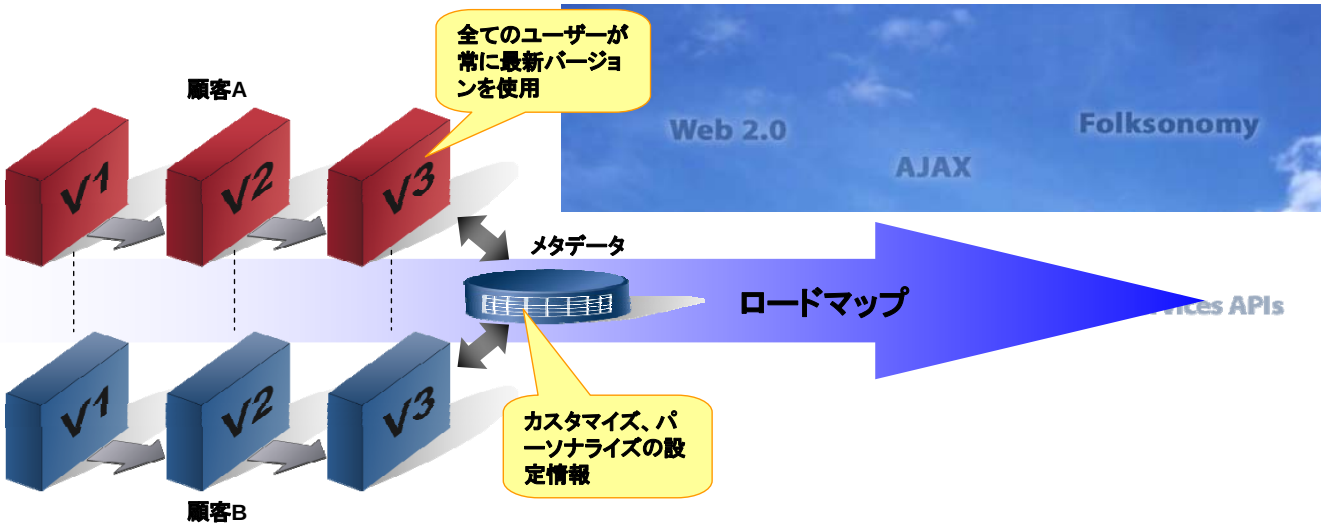
Google　ebay
salesforce　YAHOO!

- 複数のソフトウェアバージョン
- 高いメンテナンス費用
- ベンダーの技術革新（新機能）の導入が遅い

- ベンダーの技術革新（新機能）の導入が早い
- 企業の規模に合わせた拡張
- すべての顧客に高性能のインフラを提供
- 自動アップグレード

カスタマイズ情報のメタデータ化

簡単なカスタマイズとバージョンを超えた継続性



➔カスタマイズ情報は、ユーザーの労力ゼロで次のバージョンに引き継がれます
➔ベンダーは最新バージョンのみの提供／メンテナンスに注力できます
　品質・開発スピードの向上
➔ユーザーは互換性を気にすることなく、常に最新の機能を利用できます
　世界規模でベストプラクティスを共有

マッシュアップ – 新しいサービスをスピーディーに

顧客、担当者、リード情報のマッピング

IP電話連絡、電話会議、在席情報、など

いつでも最新の顧客情報に更新

➔ **ビジネスアプリケーションに新しい価値を**

IdeaExchange: コミュニティの威力

コミュニティの権利拡大

デベロッパーネットワーク

デベロッパーを支援

デベロッパーネットワーク

「次のセールスフォース・ドットコム」となるパートナーを支援

Appexchange incubators

San Mateo, CA
2007年1月開催

BusinessObjects, VerticalResponse, Hyperion, accenture, bluewolf, xactly, koral, BACKWEB, dreamfactory, RedRoller, right 90, domo, clicktools, Cloud, OpenAir, Convenos, OpSource, InsideView, invisibleCRM, RingLead, Centive, APPIRIO, Avankia, StakeWare, KP, portaga, inc., PluraPage, KAILEA networks, ELOQUA, PERVASIVE, twoconnect

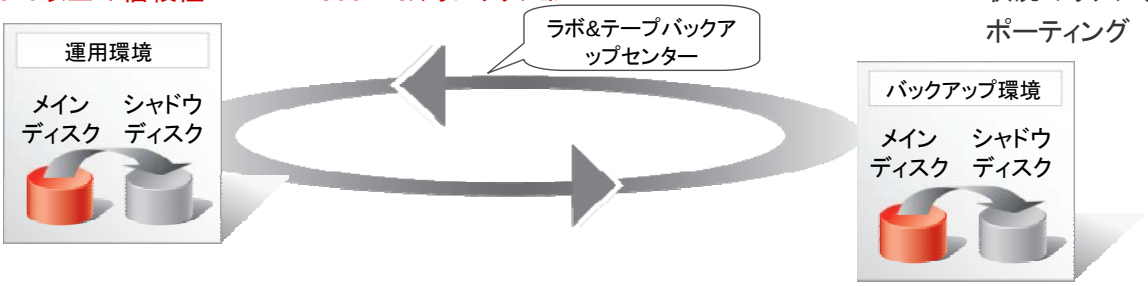
AppExchange: アプリケーションの共有と流通

マーケットプレイス

世界最高水準の情報セキュリティ

100億円を超える投資、99.9％以上の稼動実績、情報漏えい無事故
1日9,000万件を超えるトランザクション、300ms以下の処理速度

信頼性	パフォーマンス	セキュリティ	透明性
✓ ミラーリング	✓冗長性	✓SAS 70 Type II	✓情報公開
✓ 冗長性	✓通信キャリアに依存せず	✓SysTrust 認証	✓説明責任
✓ 複数のネットワーク	✓高いスケーラビリティ	✓セキュアなデータ, ネットワーク, 施設	✓リアルタイム更新
✓ 99.9%以上の信頼性	✓< 300 ms/トランザクション		✓状況のリアルタイム レポーティング



顧客の信頼を築く
trust.salesforce.com

trust.salesforce.com

Date	Number of Transactions	Avg. Speed* (seconds)	System Status						
			AP	EMEA	NA1	NA2	NA3	NA4	SSL
03/27/07	74,137,437	0.304	✓	✓	✓	✓	✓	✓	✓
03/26/07	81,583,126	0.298	✓	✓	✓	✓	✓	✓	✓
03/25/07	32,541,012	0.177	✓	✓	✓	✓	✓	✓	✓
03/24/07	31,272,014	0.154	✓	✓	✓	✓	✓	✓	✓
03/23/07	72,575,008	0.251	✓	✓	✓	✓	✓	✓	✓
03/22/07	81,029,560	0.266	✓	✓	✓	✓	✓	✓	✓
03/21/07	79,641,610	0.288	✓	✓	✓	✓	✓	✓	✓
03/20/07	79,821,237	0.291	✓	✓	✓	✓	✓	✓	✓
03/19/07	78,698,108	0.284	✓	✓	✓	✓	✓	✓	✓
03/18/07	31,872,909	0.185	✓	✓	✓	✓	✓	✓	✓
03/17/07	29,563,769	0.213	✓	✓	✓	✓	✓	✓	✓
03/16/07	68,398,084	0.257	✓	✓	✓	✓	✓	✓	✓
03/15/07	76,396,276	0.260	✓	✓	✓	✓	✓	✓	✓
03/14/07	77,246,000	0.295	✓	✓	✓	✓	✓	✓	✓
03/13/07	78,072,812	0.308	✓	✓	✓	✓	✓	✓	✓
03/12/07	79,824,902	0.318	✓	✓	✓	✓	✓	✓	✓
03/11/07	30,501,855	0.173	✓	✓	✓	✓	✓	✓	✓
03/10/07	28,961,642	0.158	✓	✓	✓	✓	✓	✓	✓
03/09/07	62,642,435	0.260	✓	✓	✓	✓	✓	✓	✓
03/08/07	75,655,731	0.259	✓	✓	✓	✓	✓	✓	✓
03/07/07	74,409,625	0.263	✓	✓	✓	✓	✓	✓	✓
03/06/07	76,575,571	0.264	✓	✓	✓	✓	✓	✓	✓
03/05/07	76,822,538	0.280	✓	✓	✓	✓	✓	✓	✓
03/04/07	31,664,784	0.172	✓	✓	✓	✓	✓	✓	✓
03/03/07	28,135,399	0.157	✓	✓	✓	✓	✓	✓	✓
03/02/07	64,134,989	0.273	✓	✓	✓	✓	✓	✓	✓
03/01/07	76,315,939	0.271	✓	✓	✓	✓	✓	✓	✓
02/28/07	76,727,671	0.281	✓	✓	✓	✓	✓	✓	✓

✓ Instance available ! Performance issues ✗ Service disruption i Informational message ? Status not available

salesforce.com Success On Demand™

MITSUBISHI 三菱電機

Changes for the Better

（第3回研究会　資料3－2）

「ASP・SaaS向け情報セキュリティ対策に関する研究会」第3回会合資料

ASP・SaaSにおける情報セキュリティ対策の現状と課題について

2007年10月17日

三菱電機株式会社
インフォメーションシステム事業推進本部
システム統括部　システム第一部
小倉 博行

1．A市／CATV通信会社様「地域情報システム」（99年4月稼動）の事例紹介（1）

●A市マルチメディアモデル整備事業（１９９８年度）

1．工事概要
　本工事では、A市内のマルチメディア化・情報化を目的として、放送（CATV）、通信（LAN）、および情報（コンピュータ）を、最新の技術（ＨＦＣ：光同軸網、ＩＰ：インターネットプロトコル、WWW：ワールドワイドウェブ、等）を駆使して融合したネットワークシステム設備（放送・通信・情報融合ネットワークシステム）を構築した。

2．工事主任技術者：**電気工事主任技術者または通信工事主任技術者**（三菱電機）

3．関連法規、検査基準、および検査官

3．１　放送設備（伝送路設備含む）
（１）関連法規　：**有線テレビジョン放送法**
（２）検査基準　：**ＣＡＴＶ技術基準（電波監理局検査基準）**
（３）社内検査官：**第一級有線テレビジョン放送技術者**（ａ社／三菱電機 ）
（４）立会検査官：監督者（A市）、監理者（ｂ社）

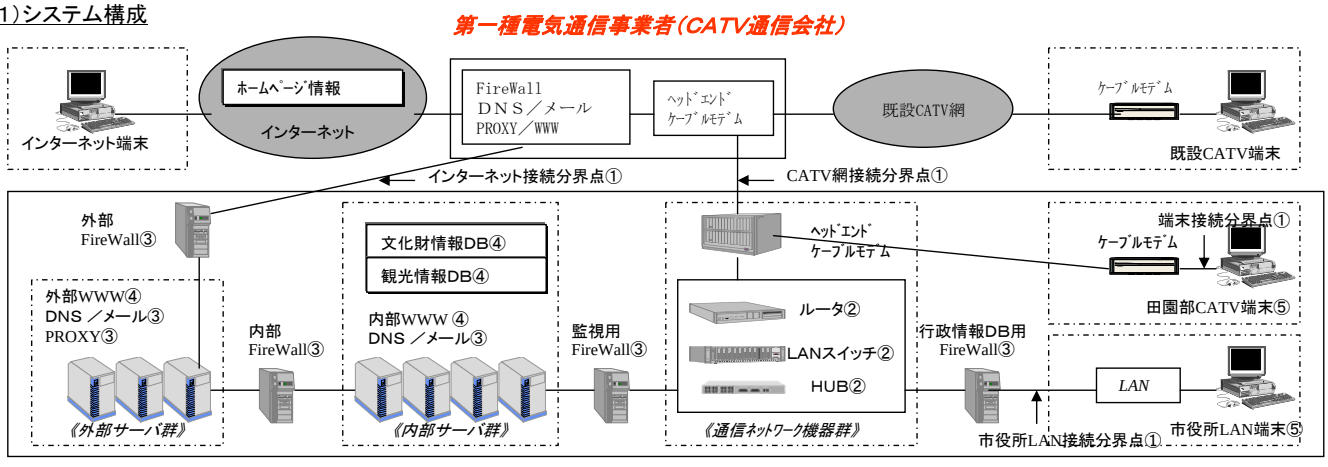
3．２　通信設備
（１）関連法規　：**電気通信事業法**
　　（第４１条 電気通信設備の維持、第４９条 端末設備の接続の技術基準）
（２）検査基準　：**郵政省令で定める技術基準（デジタルデータ伝送役務）**
（３）社内検査官：**工事担任者デジタル一種技術者**（三菱電機 ）
（４）立会検査官：監督者（A市）、監理者（ｂ社）

3．３　情報設備
（１）関連法規　：情報処理の促進に関する法律、
　　セキュリティ関連法規（刑法、建築基準法、消防法、プライバシー条例、著作権法、等）、
　　監査関連法規（商法、監査特例法、証券取引法、公認会計士、等）
（２）検査基準　：通産省監修 システム監査基準（システム開発業務実施基準）
（３）社内検査官：システム監査技術者（三菱電機）
（４）立会検査官：監督者（A市）、監理者（ｂ社）

1．A市／CATV通信会社様「地域情報システム」（99年4月稼動）の事例紹介（2）

●A市マルチメディアモデル整備事業（１９９８年度）

(1)システム構成



(2)機能

No	検査項目	検査内容
①	通信ネットワーク接続分界点検査	第一種電気通信事業者(100Base-T)および加入者(10Base-T)との接続分界点仕様の検査を行う。
②	通信ネットワーク機器検査	ルータ・ＬＡＮスイッチ・ＨＵＢのネットワーク機器の検査を行う。
③	ネットワークサーバ機器検査	FireWall、ＤＮＳ（ﾄﾞﾒｲﾝﾈｰﾑｻｰﾊﾞ）／メール、ＰＲＯＸＹ（代理応答）のネットワークサーバ機器の検査を行う。
④	アプリケーションサーバ機器検査	WWW（Ｗｅｂ－ＧＩＳ）、ＤＢ（データベース）のアプリケーションサーバ機器の検査を行う。
⑤	アプリケーションシステム動作確認	文化財情報ＤＢと観光情報ＤＢのWWW閲覧を行い、検索画面表示、地図画面表示、個別画面表示、外字表示、画像表示、および動画表示の動作確認を行う。
⑥	通信ネットワークシステム動作確認	ＣＡＴＶ端末とＬＡＮ端末からそれぞれ、参照経路（ルーティング）、ＤＮＳ参照、メールサービス、およびWWWサービス（内部、外部）の動作確認を行う。

１．Ａ市／ＣＡＴＶ通信会社様「地域情報システム」（９９年４月稼動）の事例研究

【構成員意見】

●現行の法令、仕様（認証基準）、実践のための規範（ベストプラクティス）、ガイドブック、関連・参照可能な基準、ガイドライン、、、色々な項目多すぎ、重複や抜けがあり、現場から見ると何をどこまで遵守したらよいか混乱している状況です。
●根拠法令ですら、電気通信事業法、不正競争防止法、プロバイダ責任制限法、不正アクセス禁止法、個人情報保護法、電気通信事業における個人情報保護に関するガイドライン（総務省）、Ｊ－ＳＯＸ（金融商品取引法）、Ｊ－ＳＯＸ（財務報告に係る内部統制の評価及び監査の基準）、など色々な項目があります。
●情報セキュリティＳＬＡ契約の問題は、その企業のＩＴ化の目標は何で、その効果を上げるためにISMSにどこまで費用を投入することができるかといったＩＴガバナンス（経営戦略）の問題です。Ｊ－ＳＯＸ法を中心としたＩＴガバナンスは、ITやそのプロセスにおけるリスクと費用対効果をバランスさせながら価値を付加することによって、組織目標を達成するために、組織を方向付けし、コントロールする一連の関係構造とプロセスを示しています。
●ＣＡＴＶ通信会社様の内部統制（Ｊ－ＳＯＸ）を監査法人のコンサルを受けて進行されているアプローチは正解だと考えます。
●ISO27001/2と連動した現場で理解できる『実践ガイドライン』の一本化を目指すべきであると考えます。

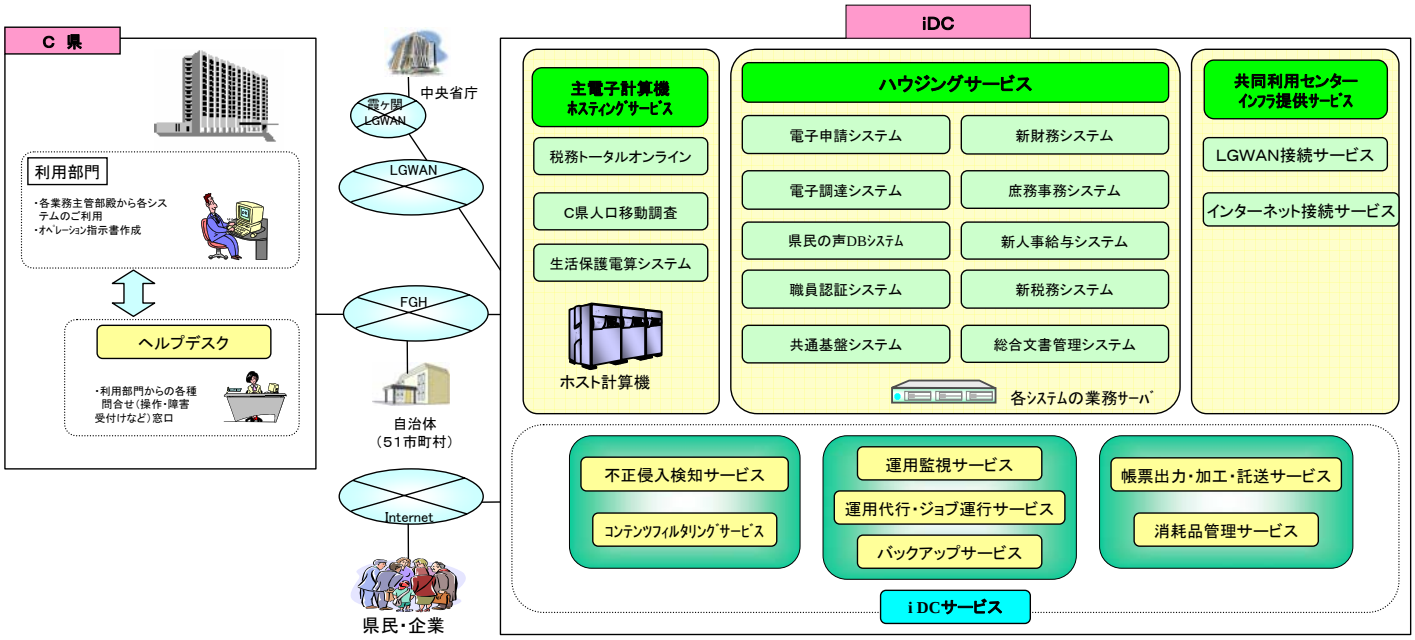
●ISO27001/2（情報セキュリティ管理）は、 ISO9001(品質管理)、 ISO14001（環境管理）に次いで、社会システムの実践規範の第三の柱に！
●ポリシー（規範）だけでは不十分で、プロセス（実践）が大切。プロセス（実践）での試行錯誤と学習が、ポリシー（規範）に跳ね返り、その再構築に役立つ。
⇒社会科学の方法論「理論と実践の好循環」（マートン[1968]）

２．Ｂ県様「電子県庁システムアウトソーシング」（０４年４月稼動）事例紹介（１）

■特徴
（１）電子申請・電子調達システムといった県民向け情報システムは元より、財務会計・人事給与・税務システムといった基幹系業務システムについても、大型電算機からサーバへのダウンサイジングに併せてiDCにアウトソーシングしている。
（２）サーバー系システムに移行できない業務システムはiDCの大型電子計算機ホスティングサービスを利用することで、福岡県は大型電算機の所有を廃止した。
（３）帳票出力業務(カット紙：500万枚/年、連続帳票：150万枚/年)、県庁への出力帳票託送についてもiDCにアウトソーシングした。
（４）上記の結果、インターネットを含め、全ての電子県庁システムの監視・運用業務を24時間365日、一元的にIDCで実施した。
■契約形態
　契約は単年度契約で、毎年、セキュリティ対策・トラブル対応・提供サービス等を細かく規定。更に、システム運用の品質条件として「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」に基づきＳＬＡ(例えばｽﾄﾚｰｼﾞ ｻｰﾋﾞｽの稼動率99.99%以上等)を受託者と協議のうえ締結。
■課題
　最近のDoSアタックや不正侵入などインターネットを介したセキュリティの脅威に対して、引き続き、的確で確実な監視体制を維持する方策。ＩＳＭＳに基づき、SLAを遵守した運用管理体制を維持する方策。

【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）

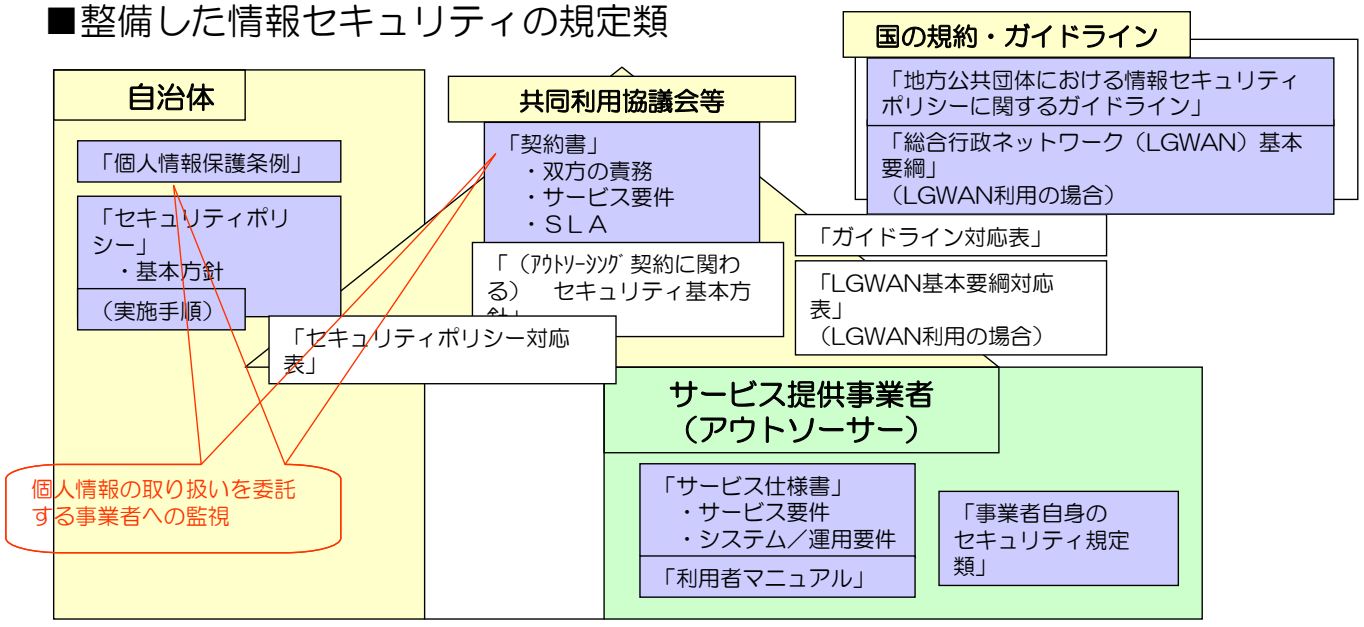
2．B県様「電子県庁システムアウトソーシング」（０４年４月稼動）事例紹介（２）



出所：(株)キューデンインフォコム資料

2．C県様「市町村共同利用電子申請システム」（０４年１０月稼動）の事例紹介（１）

■整備した情報セキュリティの規定類



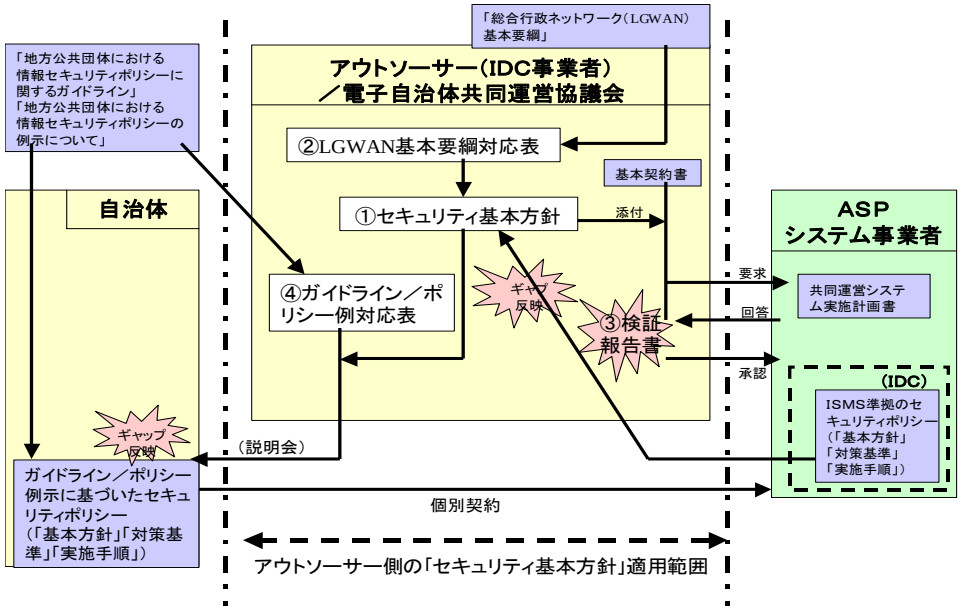
注）白地：関連する文書・規定類
　　着色：当該契約に関し整備すべきセキュリティ関連の規定類

【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）

2．C県様「市町村共同利用電子申請システム」（０４年１０月稼動）の事例紹介（２）

■アウトソーサー側の「セキュリティ基本方針」適用範囲

（注）青地文書（白地文書以外）は、既存文書を想定。



3．D県様「共同利用型電子申請受付システム」（０５年３月稼動）事例紹介

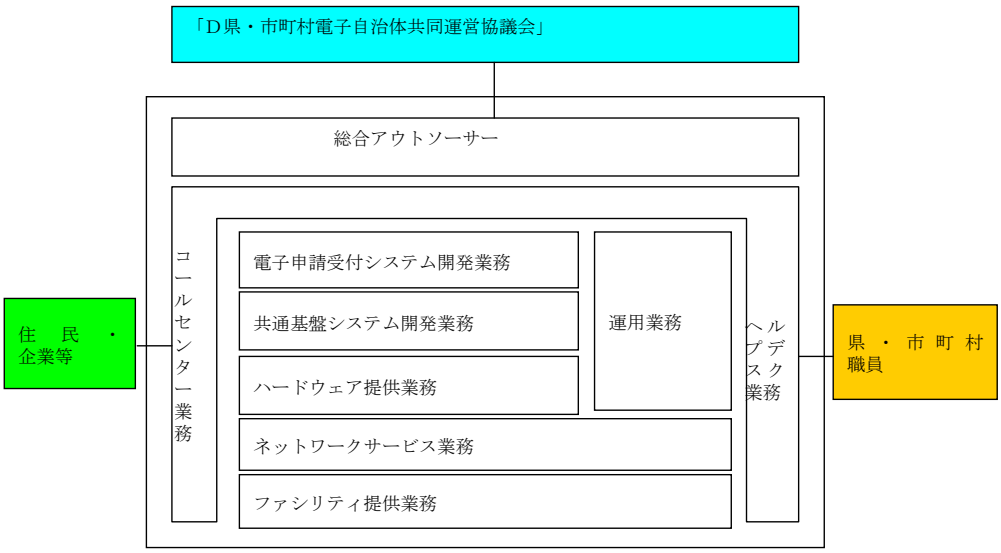
■特徴
・電子申請の実現に当たっては、業務の抜本的な見直しを図るため、BPR手順書を作成。当該手順書に基づき業務の見直しを実施している。
・申請手数料の収納にインターネットバンキングを利用(平成17年12月)。
・携帯電話申請機能を実装。運用開始は平成18年3月。
■経緯
・サービス提供に必要となる高度なファシリティ、セキュリティを有するサーバ設置スペースの確保（ハウジングサービス）および、サーバやネットワークのシステムの運用管理等については、専門事業者へアウトソーシングした。
■契約形態
・「県・市町村電子自治体共同運営協議会」を代表するD県と企業体（３社）間による業務委託契約（複数年契約）。
・当該契約とは別にSLA契約を締結。※総事業費（システム構築経費（ハード・ソフト）、運用経費等）の1/2を県が負担、残りの1/2を各市町村が人口割で負担。
■課題・各自治体の庁内業務の効率化を促進する文書管理システム、統合型GISの県・市町村共同開発・運用を目指している。

●ＳＬＡの管理・運用の留意事項
ア　ＳＬＡ設定値
　ＳＬＡ設定値は、住民用（２４時間・３６５日）と職員用（勤務時間帯）とで、コスト・パフォーマンスを考慮した上げ下げを行なう。
イ　ＳＬＡの見直し、再設定
　自治体ではＳＬＡ数値化は困難なので、ASPIC「実践の手引き」等を参照して設定する。特に、業務システムのＳＬＡは実例が少ないので、実績値に基づく見直しや他自治体との比較が必要であり、毎月の報告会や毎年の検討会等でＳＬＡの見直し再設定を行なう。
ウ　ＢＰＲ（業務プロセス革新）
　自治体の行財政改革（ＩＴによる構造改革）を目的として、システムの単なるＳＬＡ数値の見直し再設定をするのではなく、業務自体の抜本的見直しを行なうＢＰＲ（業務プロセス革新）や経営評価指標KPI（Key Performance　Indicator）の見直しを行い、ＥＡ（業務・システム全体最適化）に基づく、住民サービス向上・経費削減を行なう。

【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）

3．D県様「共同利用型電子申請受付システム」（０５年３月稼動）事例紹介

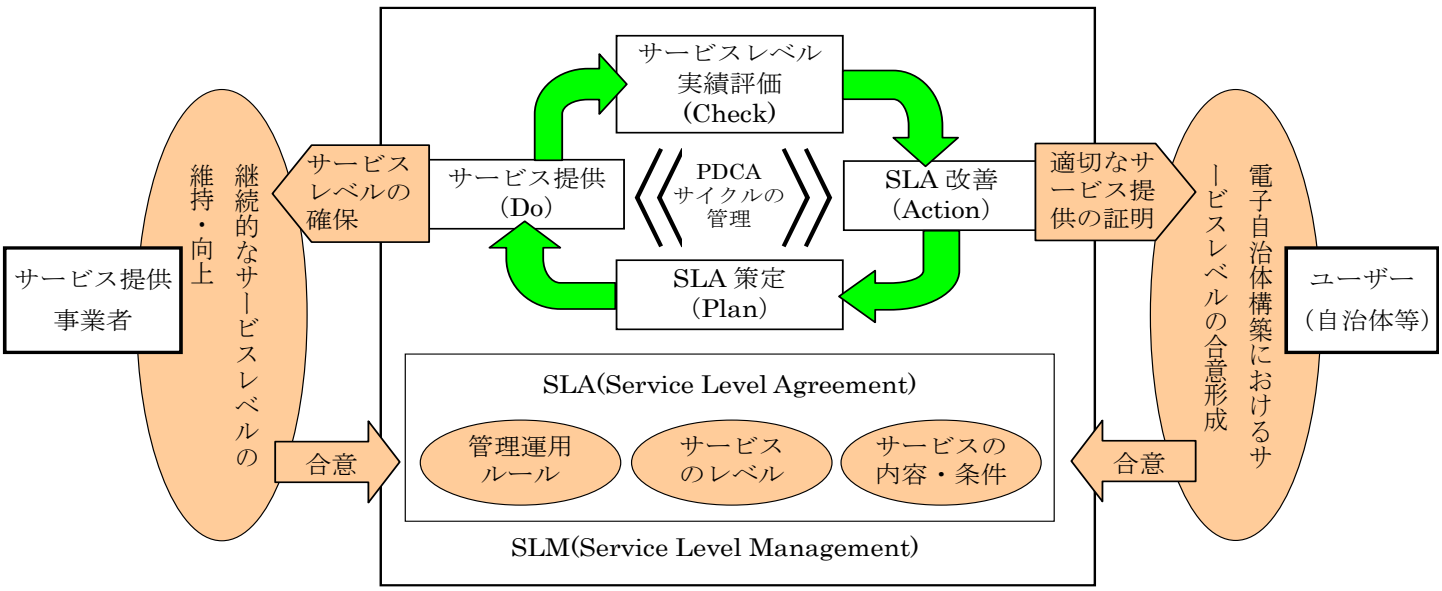
D県共同利用型電子申請受付システム概要図



【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）

MITSUBISHI 三菱電機　Ⅰ　ASP・SaaSにおける情報セキュリティ対策の現状　Changes for the Better

3．D県様「共同利用型電子申請受付システム」（０５年３月稼動）事例紹介



【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）P.65

4．電子自治体構築に関連する基準や認証制度

●情報セキュリティマネジメントの実践のための規範⇒「政府機関の情報セキュリティ対策のための統一基準(第2版)」：政府機関全体としての情報セキュリティ水準の向上を図るために策定された「政府機関統一基準」の改訂（平成19年6月14日「情報セキュリティ政策会議」（議長：内閣官房長官）決定）

■情報セキュリティ監査ガイドライン　⇒ISO/IEC27002（JIS X 5080）

- 自治体のセルフチェックを重要視している「実践ガイドライン」

地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書（平成15 年12 月25 日総務省）
⇒JIS X 5080と整合をとり、「報告書」の別添1 管理基準（975項目）、別添2 セルフチェックリスト（258項目）、またはLASDEC「やってみよう　情報セキュリティ　内部監査」（80項目）⇒仮説ビデオ

■ISMS （情報セキュリティマネジメントシステム）　⇒ISO/IEC27001

■プライバシーマーク制度　⇒ JIS Q15001

- 個人情報の適切な保護・管理を実施している事業者を認定
- 特に住民の個人情報に関わるシステムを委託するASP・IDC事業者は、取得が望ましい

■ ISO/IEC 15408　⇒ＳＴ確認

- 製品やシステムがあるレベルのセキュリティ要件を満たしていることを認証するための評価基準

■ ITIL （IT Infrastructure Library）　⇒ISO/IEC20000

- ベストプラクティス（参考にすべき先行事例集）

【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引きP.140～144」（2006年）

●セキュリティ対策を含むASP・SaaSのアーキテクチャ設計の必要性

情報セキュリティマネジメントシステム（ISMS）が規定する安全性【機密性、完全性、可用性】の個別最適化だけでなく、信頼性【完全性、正確性、正当性、継続性】を加えた全体最適化に結びつくITガバナンス技術体系への展開を見据えた情報セキュリティ・アーキテクチャ（政府CIO連絡会議決定に準拠）を設計する。
なお、上記アーキテクチャは、運用プロセスITIL（ISO/IEC20000）、情報セキュリティ管理ISMS（ISO/IEC27000、JISX5080）、内部統制（IT全般統制）COBITといった国際標準に基づくITガバナンス機能要件に準拠することが前提。
ASP・SaaSは、ITIL（ISO/IEC20000）に基づく高品質・可視化された運用プロセスを実現し、「情報」の安全性（機密性、完全性、可用性）と信頼性（完全性、正確性、正当性、継続性）の各リスクをバランスさせながらコントロールする「ASP・SaaSのシステム構造」上でアプリケーションソフトウェア「機能」が動作する。
（注）システム生産標準規格COBIT（Control Objectives for Information and related Technology）は「情報関連技術のコントロール目標」の略であり、「情報通信技術に関連したリスクや便益を認識し、マネジメントすることを支援するよう、ITガバナンスを躍進させるツール」として、情報セキュリティ管理システムISMSの３つの情報基準を含む７つの情報基準（有効性、効率性、機密性、完全性、可用性、準拠性、信頼性）の全体最適化するようデザインされている。

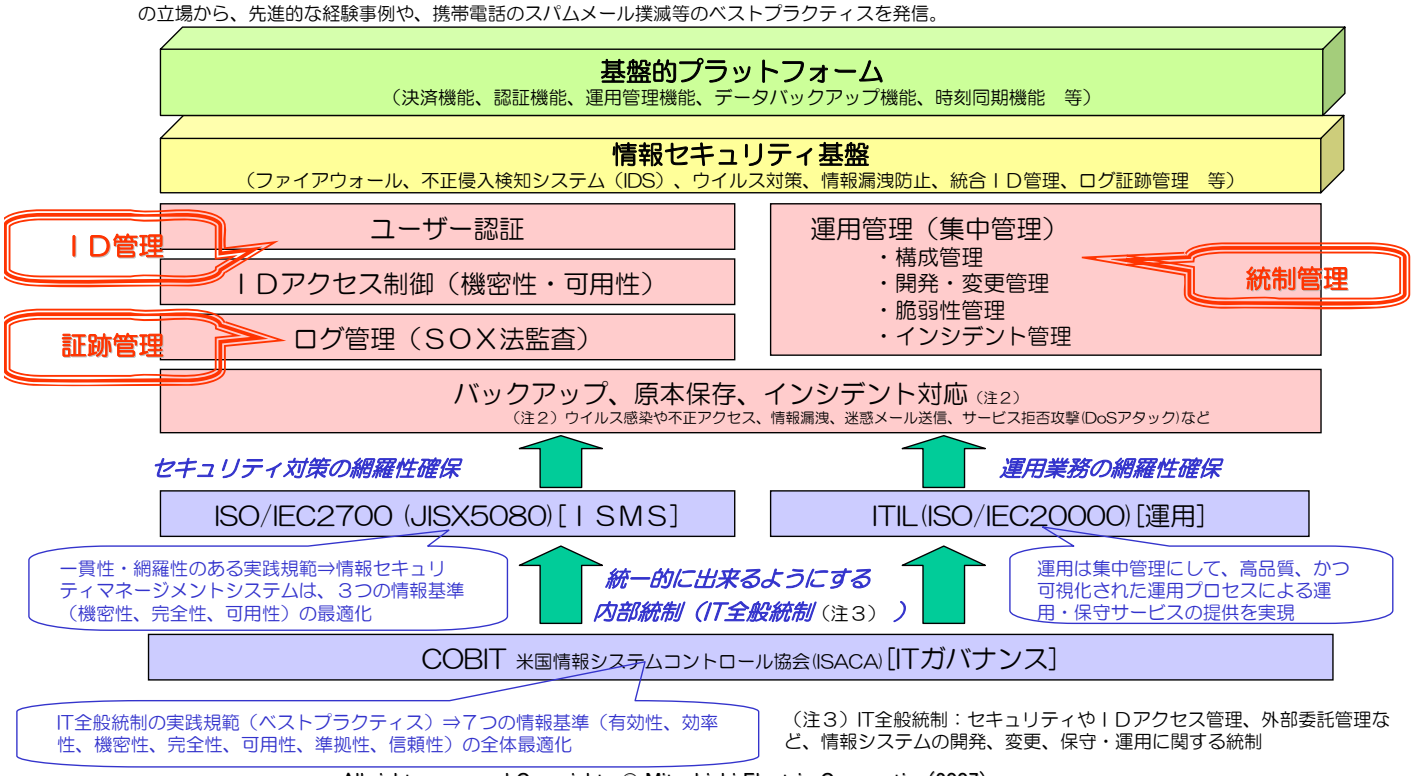
コンプライアンス（ＩＴガバナンス）

安全性 （機密性、完全性、可用性）	信頼性 （完全性、正確性、正当性、継続性）

システムアーキテクチャ
（アプリケーション、ネットワーク、ソフトウェア、ハードウェア、運用、セキュリティ）

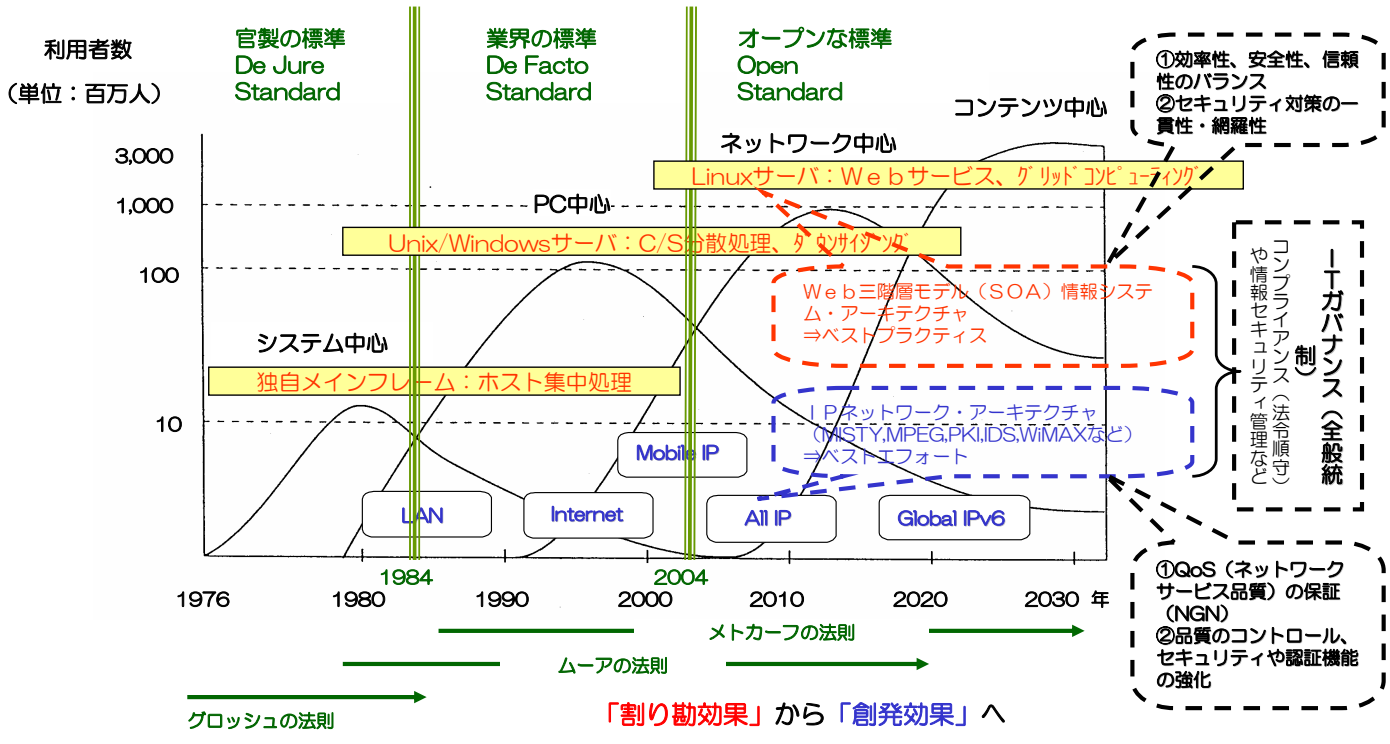
●国際標準に基づくＩＴガバナンス（注１）の機能要件

（注１）ＩＴガバナンス：ITやそのプロセスにおけるリスクと費用対効果をバランスさせながら価値を付加することによって、組織目標を達成するために、組織を方向付けし、コントロールする一連の関係構造とプロセス。2006年10月、アテネにて開催された、第1回国連IGF(ｲﾝﾀｰﾈｯﾄ･ｶﾞﾊﾞﾅﾝｽ･ﾌｫｰﾗﾑ)では、インターネットのアクセス、開放性、セキュリティ、多様性について議論。日本経団連が、第1回IGFにミッションを派遣し、産業界の立場から、先進的な経験事例や、携帯電話のスパムメール撲滅等のベストプラクティスを発信。



（注３）IT全般統制：セキュリティやＩＤアクセス管理、外部委託管理など、情報システムの開発、変更、保守・運用に関する統制

●ネットワーク中心時代の情報セキュリティガバナンス

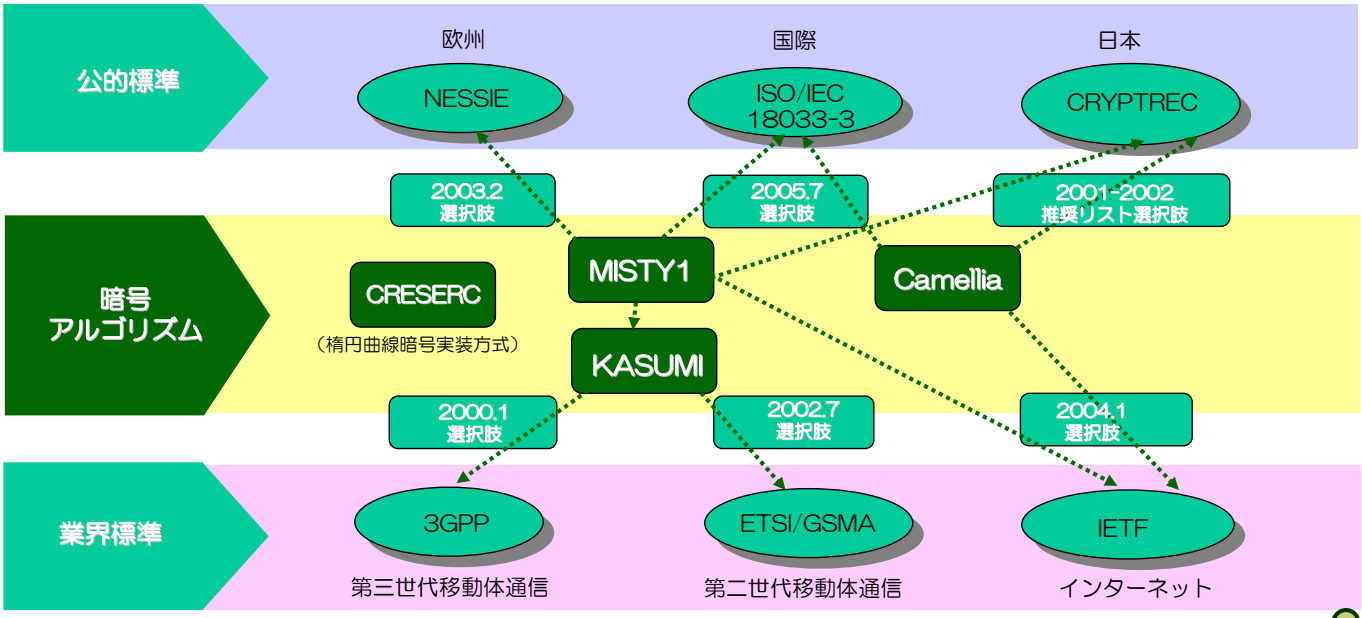


出典：David Moschella, “Waves of Power”，1997 / 02 に加筆（2004年総務省「ユビキタスネット社会の実現に向けた政策懇談会」村上篤道 三菱電機役員技監）資料をもとに作成

●実証済みのＷｅｂサービスシステム構築モデル（オープン化・Ｗｅｂ化・インターネット化を前提としたシステムの情報システム構造）に基づく、セキュリティ・アーキテクチャの実装設計を行って、一貫性・網羅性のある多層的な情報セキュリティ対策を行うことが必要

	ウィルス/ワーム	侵入	不正アクセス	情報漏えい	改ざん	盗聴
全般	セキュリティポリシーの利用者への啓蒙・教育					
	セキュリティ設計・ST確認					
	運用監査					
	識別コード・パスワード管理					
			証跡の保存・分析			
ネットワーク	不審な通信の検知・遮断					
		ファイアウォールによるフィルタリング・ゾーニング			通信の暗号化	
		IPSによる通信監視				
		通信ログ取得				
		脆弱性診断				
サーバ	ウィルス対策		入退出管理	メール監査	改ざん検知	
		セキュリティパッチ			重要データの暗号化	
			ログ取得			
		脆弱性診断				
アプリケーション		脆弱性診断				
			利用者の認証とアクセス制御		原本管理	
			アプリケーションログの取得			
クライアント	接続機器の適性検査・検疫					
	ウィルス対策		利用者認証			
		セキュリティパッチ		入出力デバイス制限		
			操作ログの取得			

（1）暗号アルゴリズムの標準化状況（MISTY、KASUMI、Camelliaなど）



弊社は、MISTY、KASUMI、Camelliaなど世界最高水準の暗号技術を開発しました。この暗号技術をベースに、耐タンパ実装技術（不正アクセスから鍵を保護する技術）、携帯端末や自動車用電子機器等への組込みセキュリティ技術、ネットワーク経由の攻撃を検知・遮断するネットワークセキュリティ技術などの研究開発を行っています。

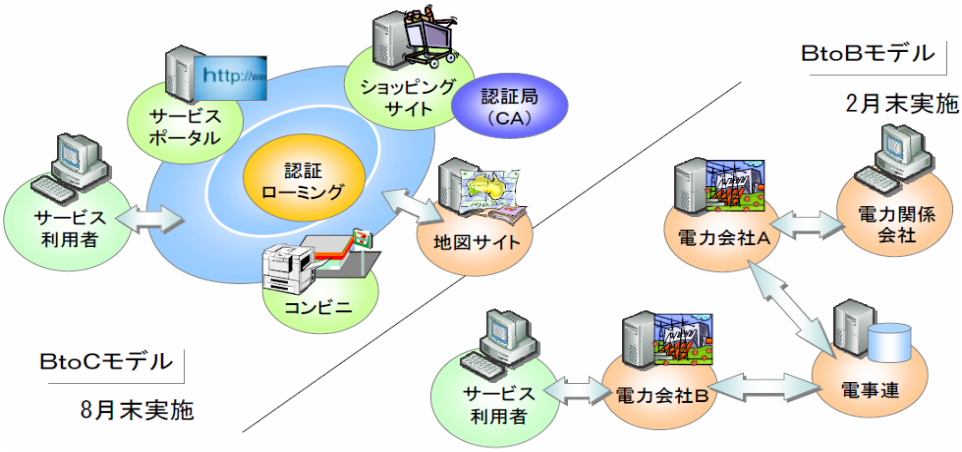
（独）情報通信研究機構（ＮＩCT）委託研究

（２）「異なるCA間の認証ローミング技術に関する研究開発」

- NICT委託研究として平成１７年度・平成１８年度の２年計画で実施
- 三菱電機株式会社と株式会社テプコシステムズ（幹事企業）の共同研究
- 実施計画上の課題は、以下の２点

①異なるＣＡ間でアイデンティティ情報の受け渡しが発生しない高速かつ安全な認証方式の開発（三菱電機担当）

②上記認証方式を実環境で有効に機能させるための実証実験（テプコシステムズ担当）

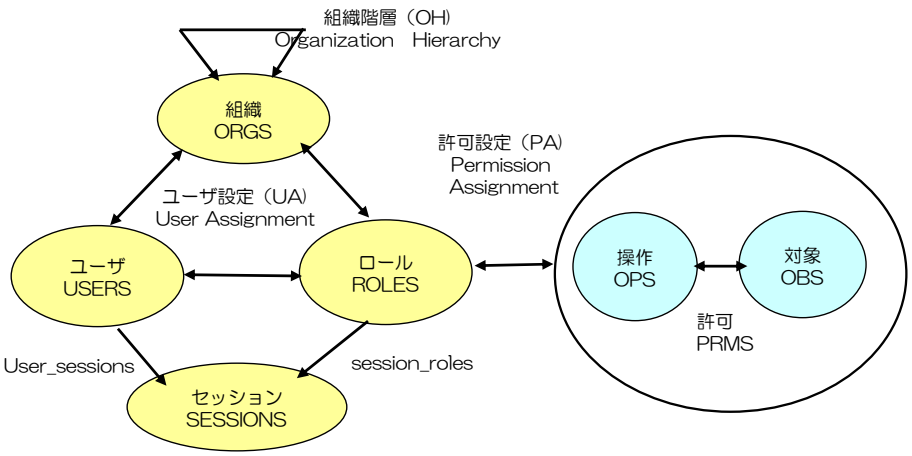


【出典：総務省「地域情報プラットフォームフォーラム」,http://www.applic.or.jp/seminar/pfforum2006/】

 60

MITSUBISHI 三菱電機　Ⅲ　オープンな標準の情報セキュリティ製品・技術開発　Changes for the Better

（３）国際標準(NIST)ロールベースアクセス制御（RBAC）システム MistyGuard〈MissionCore〉

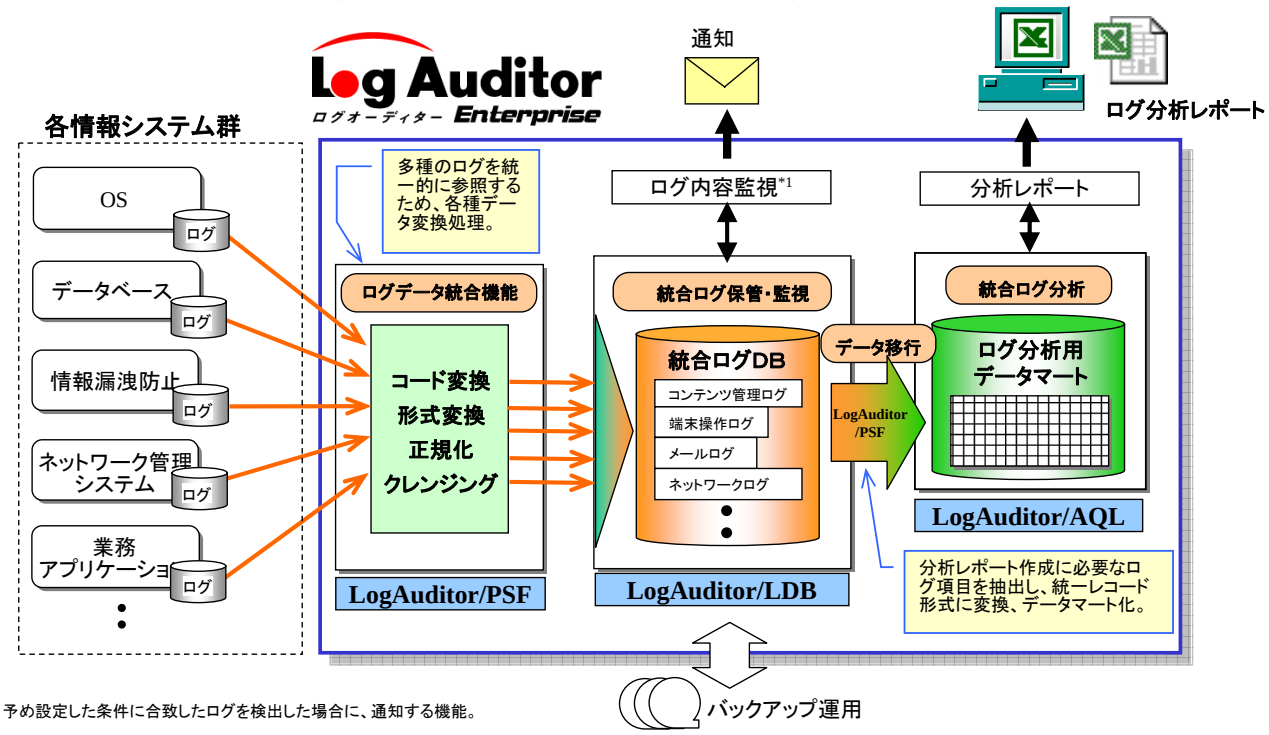


国際標準(NIST)ロールベースアクセス制御（RBAC:Role-Based Access Control）モデル

 61

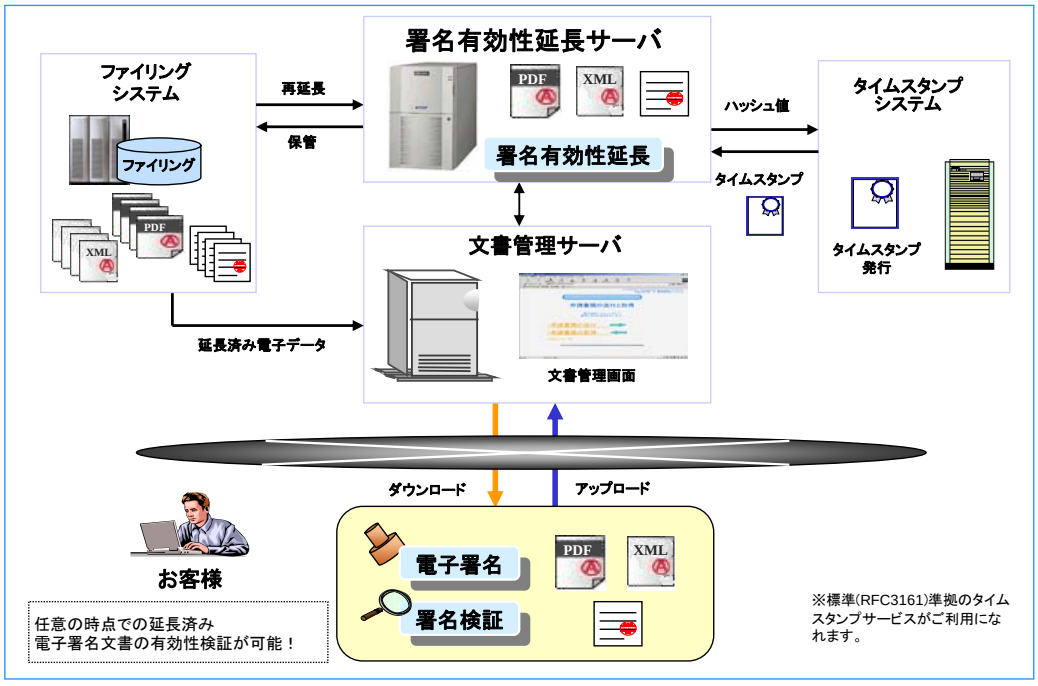
（4）三菱統合ログ管理・分析システム　MistyGuard〈LogAuditor〉

- ✓ 統合ログ管理・分析システムとして、LogAuditor Enterpriseをご提供。
- ✓ 多種大容量のログを統合し、高速に検索・集計した結果をMicrosoft Excel等にレポート出力するシステム。



*1：予め設定した条件に合致したログを検出した場合に、通知する機能。

（5）三菱署名有効性延長システム　MistyGuard＜EVERSIGN＞ ⇒文書ファイルの原本の真性を確認する電子署名長期保存技術（RFC3126準拠モデル）



総務省　ASP・SaaS情報セキュリティ対策研究会　第3回会合資料

ASP・SaaSにおける情報セキュリティ対策の現状と課題について

BLAYN HTTP://WWW.BLAYN.CO.JP/ BRILLIANT LEGEND ARE YOURS NOW

BLAYN BRILLIANT LEGEND ARE YOURS NOW

ブレインとは 【会社概要】

会社名　　ブレイン株式会社

住所　　本　　社：東京都渋谷区道玄坂1-20-2　石橋ビル2F
上海支社：上海市浦東新区龍陽路 1880 号万邦花園 6

事業内容　　メールソリューションに特化したソフトウェアライセンスの
企画・開発・販売

資本金　　1,800万円

代表取締役　　天毛　伸一　（テンモウ　シンイチ）

従業員数　　30名

ブレインが提供するサービス

メールサービスに100%特化 ブレインは、インターネットのメールという分野にサービス特化したソフトウェアメーカーです。

4types of software
BLAYN MAIL / UNION MAIL / BLAYN ENGINE / BLAYN DATABASE

blaynmail 導入実績2000社のメール配信システム。

unionmail 複数メンバーでメールを共有管理。
メール共有受信システム。

blaynengine 携帯メールに確実に届く。
携帯電話向けのメール配信に特化した
業界最安値のメール配信エンジン。

Continure・・・

本日ご紹介するサービスモデル

【ブレインメール】

メール配信ASPサービスとして

7年前より提供

導入先は2,000社
（OEM提供等含む）

ミニマムプランは月額2,000円

ブレインメールのセキュリティ対策

プライバシーマーク

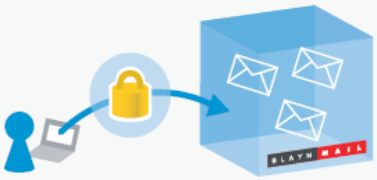
A821806(01)

社員教育、監査の実施、システム面、社内組織など多数の項目において個人情報を適切に保護している事が第三者機関より認定されていますので、安心してご利用いただけます。

安心のサポート体制

ブレインメールは自社開発・自社運用のメリットを生かし、社内にお客様専用サポート窓口をご用意しておりますので、第三者にお客様のお問合せ内容が伝わることはございません。

情報の暗号化



文字情報を暗号化することにより、電子メールによる個人情報流出のリスクを減らし、適切な安全管理を行っています。
また、ブレインメールは配信パフォーマンスを落とすことなく安全な暗号化メールの送信を実現しました。

日本ベリサイン社のセキュアシールIDを取得

ブレインメールは現在最も信頼性の高い、SSLと呼ばれる暗号通信技術を採用し、お客様のパソコン、携帯から送信される情報の秘匿性を高めております。
第三者機関である日本ベリサイン社のセキュアシールIDは安全な通信の証明です。

ブレインメールのセキュリティ対策

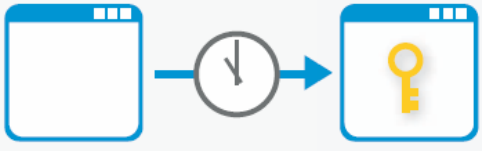
ログイン認証

お客様専用のログインID及びパスワードにて管理を行っています。

ページ毎アクセス制限

ページ移動毎に認証を掛けることにより、直接アクセスを遮断するセキュリティー体制を整えております。

自動ログアウト



一定時間において操作が無い場合は自動的にログアウトします。

※今後の予定

ISMSの取得（2008年度予定）

資料Ⅰ－3

情報セキュリティ対策に関連する
既存の基準・ガイドライン

目次

情報セキュリティに関する既存の法令・基準・ガイドライン等

1. 情報セキュリティに関する分野

- JIS Q 27001 :2006
- MICTS（情報及び通信技術セキュリティの管理）
- NIST（米商務省標準技術局）
- プロバイダ責任制限法（平成13年法律第137号）
- 不正アクセス禁止法（平成11年法律第128号）
- JIS Q 27002 :2006
- FISC（金融情報システムセンター）
- 電気通信事業法（昭和59年法律第86号）
- 不正競争防止法（平成5年法律第47号）

2. 個人情報保護に関する分野

- JIS Q 15001 :2006
- 個人情報保護法（平成15年法律第57号）
- 電気通信事業における個人情報保護に関するガイドライン（平成16年8月31日総務省告示第695号）

3. 内部統制に関する分野

- COBIT（IT Governance Institute）
- SysTrust（米国公認会計士協会）
- WebTrust（米国公認会計士協会）
- SAS70（米国公認会計士協会）
- 金融商品取引法（昭和23年法律第25号）
- 財務報告に係る内部統制の評価及び監査の基準（金融庁）

4. SLAに関する分野

- 電子自治体 基幹系SLA設定例（ASPIC Japan）
- 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）
- 民間向けITシステムのSLAガイドライン（第3版）（日本情報技術産業協会（JEITA））
- 情報システムに係る政府調達へのSLA導入ガイドライン（経済産業省）

5. ITサービスに関する分野

- ISO/IEC 20000-1 :2005
- PD0005 PD0015
- ISO/IEC 20000-2 :2005
- ITIL

6. 事業継続に関する分野

- BS 25999（英国規格協会）
- 事業継続ガイドライン（第1版）（内閣府防災担当）
- 事業継続計画策定ガイドライン（経済産業省）
- 中小企業BCP策定運用方針（中小企業庁）
- 金融機関等におけるコンティンジェンシープラン策定のための手引書（FISC）

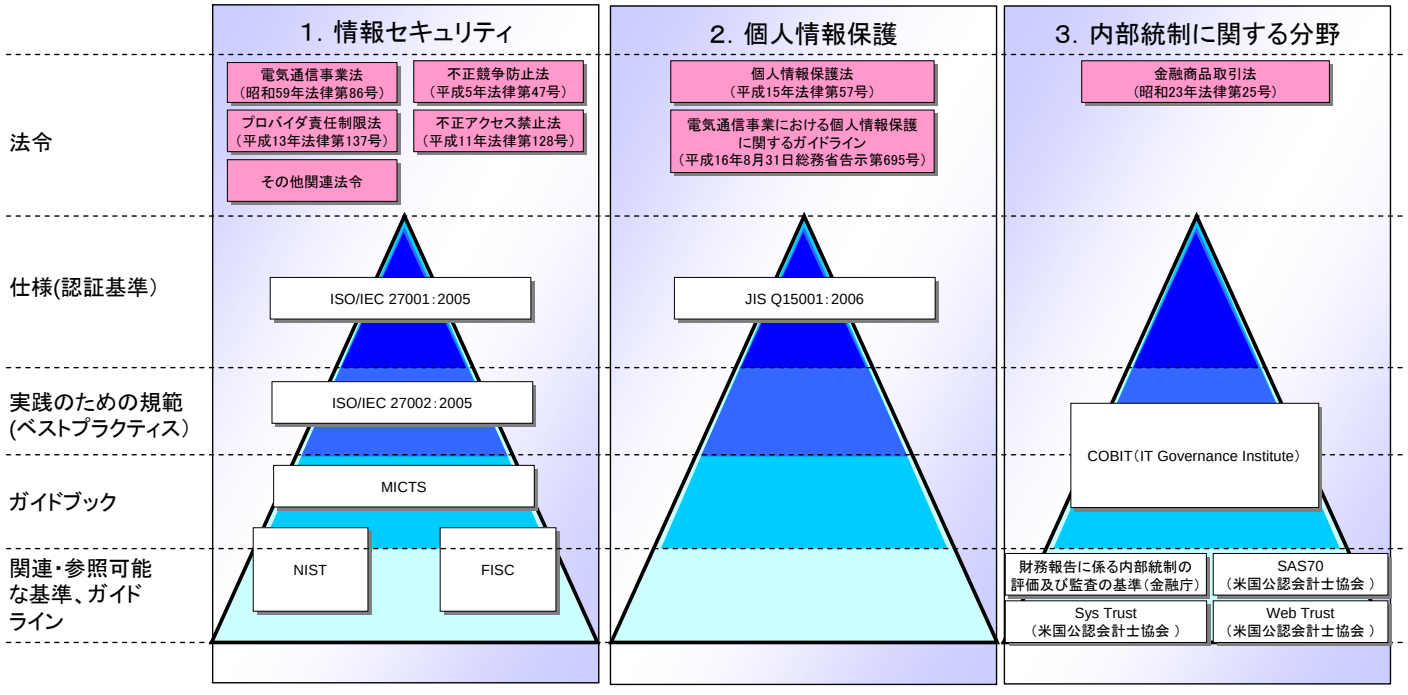
7. 信頼性に関する分野

- 情報通信ネットワーク安全・信頼性基準（昭和62年郵政省告示第73号）

凡例：法令（法律、告示、省令を含む） ガイドライン

情報セキュリティ等の各分野と既存の基準・ガイドラインとの対応関係の整理 ①

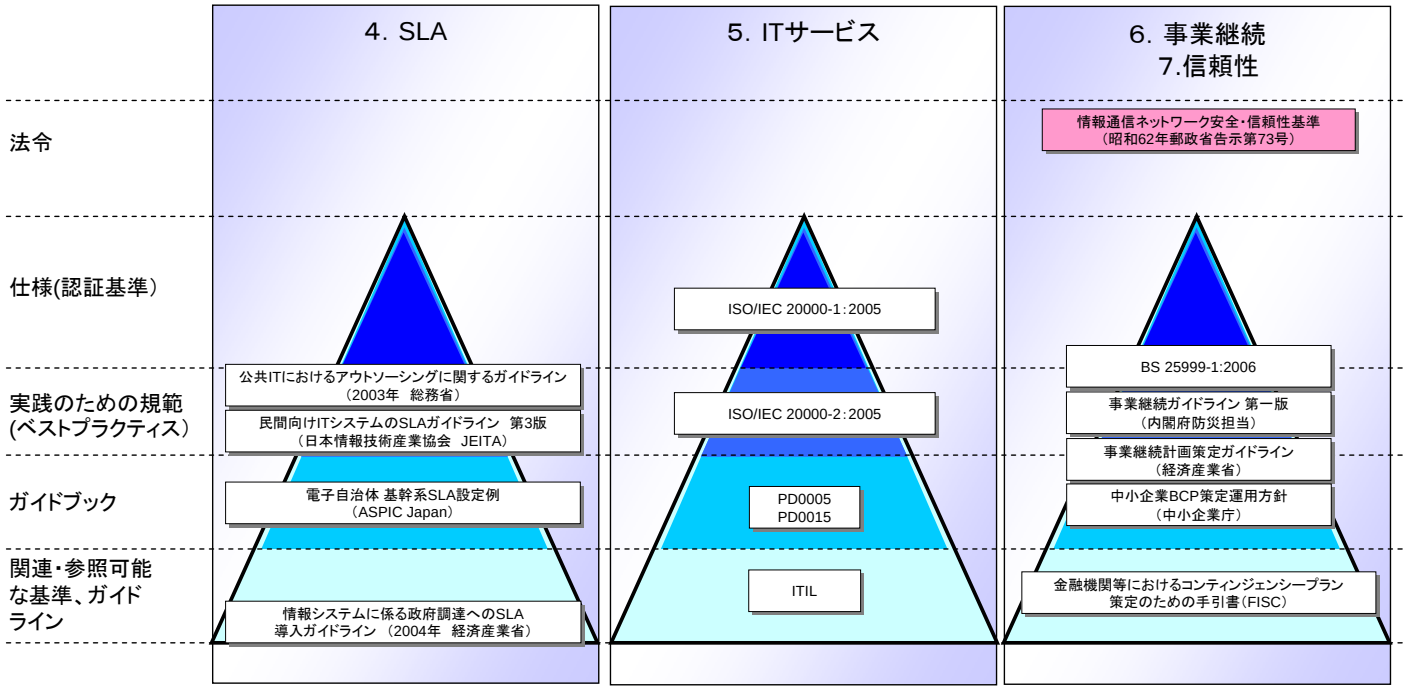
情報セキュリティ、個人情報保護、内部統制の各分野において、法令、基準、ガイドラインの位置関係は以下の通り。



凡例：法令（法律、告示、省令を含む） ガイドライン

情報セキュリティ等の各分野と既存の基準・ガイドラインとの対応関係の整理 ②

SLA、ITサービス、事業継続性、信頼性の各分野において、法令、基準、ガイドラインの位置関係は以下の通り。

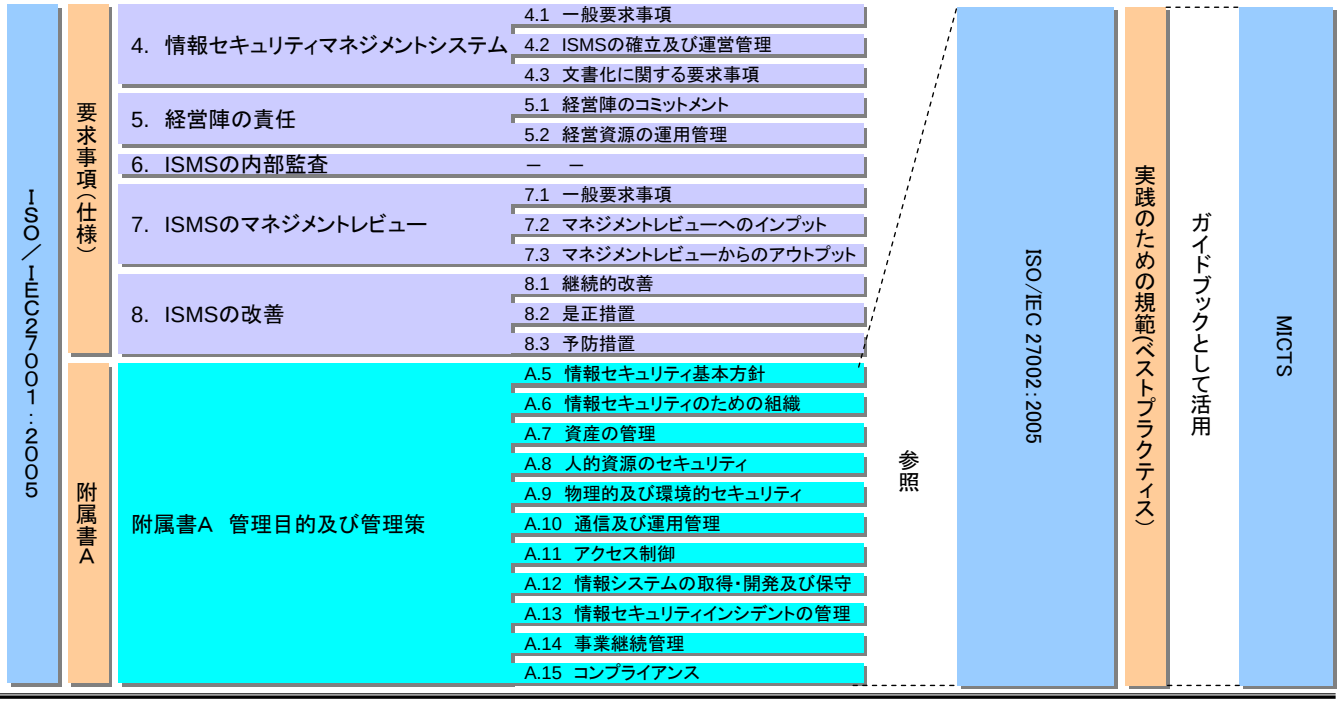


凡例：　法令（法律、告示、省令を含む）　ガイドライン

参考資料

1. 情報セキュリティ分野に関する既存の基準・ガイドラインの構造

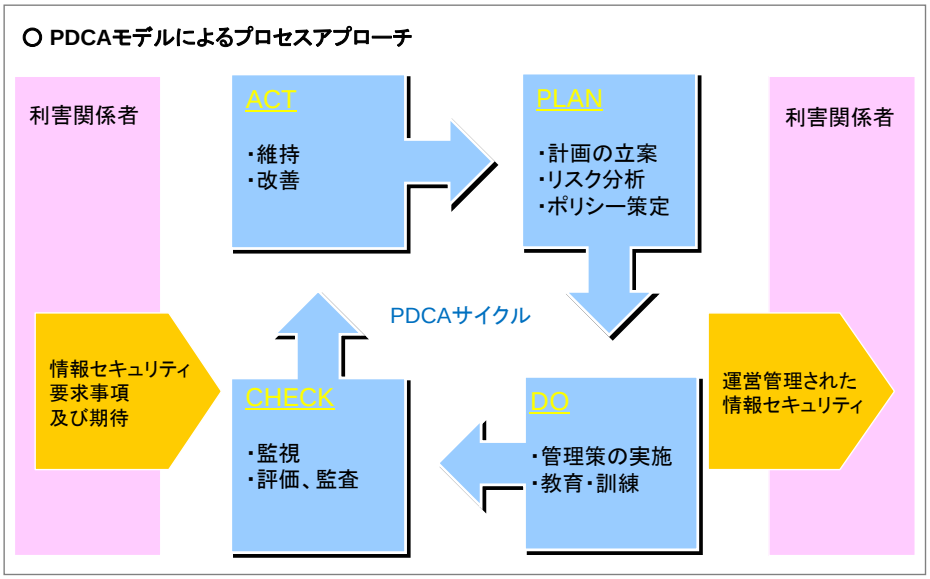
ISO/IEC27001は、情報セキュリティマネジメントシステム構築に際して組織が遵守すべき要求事項（仕様）と附属書A（管理策）からなり、ISO/IEC27002は、附属書Aのベストプラクティスを集めたガイドラインとして位置付けられる。MICTSは、ISO/IEC27000シリーズのガイドブックとして位置付けられており、将来、ISO27000シリーズへ組み込まれる予定。（一部組み込み済み）



（参考）ISO/IEC 27001:2005の概要

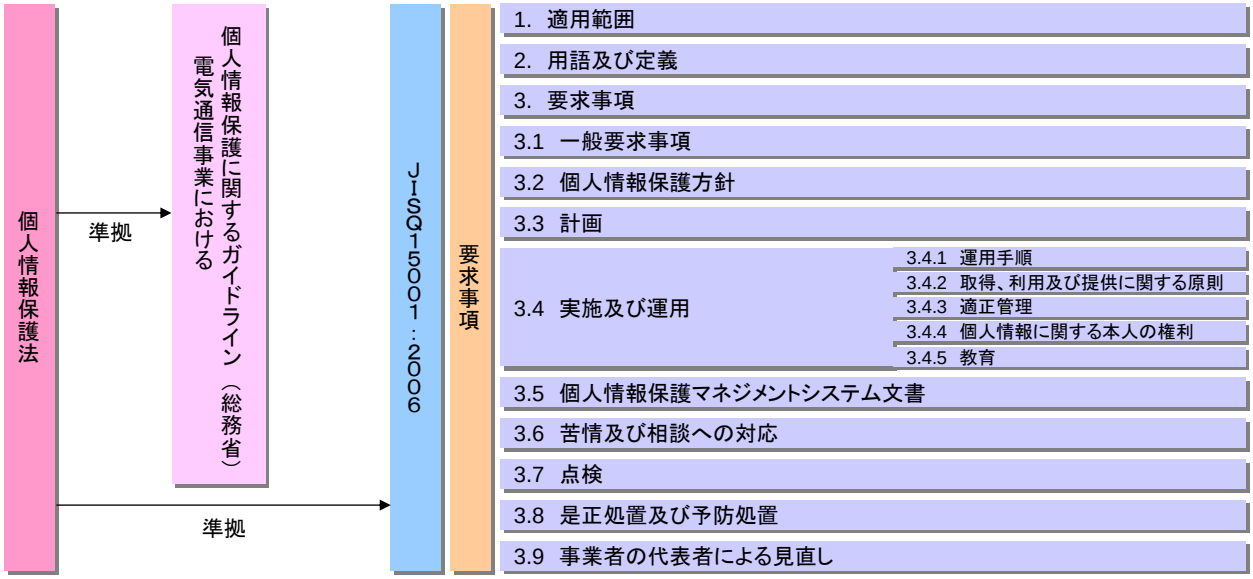
ISO/IEC 27001は情報セキュリティマネジメントシステムの要求事項として、組織が所有する情報資産を機密性・完全性・可用性の観点から適切管理するための包括的な枠組みを提供している。コンピュータシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針（情報セキュリティポリシー）や、それに基づいた具体的な計画、その実施と運用、一定期間毎の運用の評価や見直しまでを含めたトータルなセキュリティ管理体系の構築を要求している。

ISO/IEC 27001の原型はBS 7799であり、Part1（ガイド）とPart2（認証基準）で構成され、BS 7799のPart2はISO/IEC 27001、Part1はISO/IEC 27002として国際規格化されている。ISMS適合性評価制度においては、第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価する基準として使用されている。



2. 個人情報保護に関する既存の基準・ガイドラインの構造

個人情報保護分野に関する既存の基準・ガイドラインの構成・章立て及び関係は、以下のように整理される。



（参考）個人情報保護法の概要

個人情報保護法（平成15年法律第57号）は、全56条に附則が付けられており、第1章から第3章までが個人情報保護の基本法部分を構成し、第4章以下は民間部門を対象として具体的な権利義務を規定した一般法部分となっている。

第一章　総則
　第一条（目的）
　第二条（定義）
　第三条（基本理念）

第二章　国及び地方公共団体の責務等

第三章　個人情報の保護に関する施策等

　第一節　個人情報の保護に関する基本方針

　第二節　国の施策

　第三節　地方公共団体の施策

　第四節　国及び地方公共団体の協力

第四章　個人情報取扱事業者の義務等

　第一節　個人情報取扱事業者の義務
　　第十五条（利用目的の特定）
　　第十六条（利用目的による制限）
　　第十七条（適正な取得）
　　第十八条（取得に際しての利用目的の通知等）
　　第十九条（データ内容の正確性の確保）
　　第二十条（安全管理措置）
　　第二十一条（従業者の監督）
　　第二十二条（委託先の監督）
　　第二十三条（第三者提供の制限）
　　第二十四条（保有個人データに関する事項の公表等）
　　第二十五条（開示）
　　第二十六条（訂正等）
　　第二十七条（利用停止等）
　　第二十八条（理由の説明）
　　第二十九条（開示等の求めに応じる手続）
　　第三十条（手数料）
　　第三十一条（個人情報取扱事業者による苦情の処理）
　　第三十二条（報告の徴収）
　　第三十三条（助言）
　　第三十四条（勧告及び命令）
　　第三十五条（主務大臣の権限の行使の制限）
　　第三十六条（主務大臣）第三十六条

　第二節　民間団体による個人情報の保護の推進

第五章　雑則

第六章　罰則

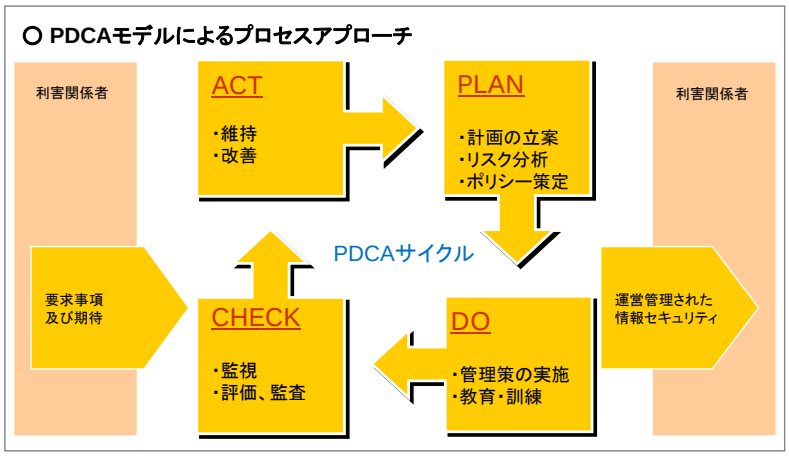
　第五十六条
　第五十七条
　第五十八条
　第五十九条

附　則　抄

（参考）JIS Q15001：2006の概要

JIS Q 15001は個人情報保護マネジメントシステムの要求事項として、事業者が所有する個人情報を特定し、その入手から廃棄に至る一連の個人情報の取扱いを適切管理するための包括的な枠組みを提供している。コンピュータシステムに保存されている個人情報のみならず、記録媒体や紙媒体等を含めた個人情報を扱う際の基本的な方針（個人情報保護方針）や、それに基づいた具体的な計画、その実施と運用、一定期間毎の運用の評価や見直しまでを含めたトータルな個人情報保護管理体系の構築を要求している。

JIS Q 15001はOECDプライバシーガイドラインの影響を大きく受けており、個人情報保護法施行後に規格の改定が行われJIS Q 15001:2006として同法律との親和性が一層高まった内容になっている。プライバシーマーク制度においては、第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価する基準として使用されている。



（参考）JIS Q15001：2006の個人情報保護法への対応

JIS Q15001は、もともとOECDのプライバシーガイドラインの影響を受けて策定されたものである。その後、新規格JIS Q15001:2006として個人情報保護法との親和性が一層高まっている。本規格を遵守することで、個人情報保護法も遵守することができるようになっている。基本的な枠組みは、ISO/IEC27001と同様にPDCAサイクルの運用になるが、3、4.3.1、4.4、4.6章には、個人情報保護分野特有の基準が設けられている。

1 適用範囲
2 引用規格
3 用語及び定義
4 要求事項
4.1 一般要求事項
4.2 個人情報保護方針
4.3 計画
4.3.1 個人情報の特定
4.3.2 法令、国が定める指針及びその他の規範
4.3.3 リスクなどの認識・分析及び対策
4.3.4 資源、役割、責任及び権限
4.3.5 内部規程
4.3.6 計画書
4.3.7 緊急事態への準備
4.4 実施及び運用
4.4.1 運用管理
4.4.2 取得・利用及び提供に関する原則
4.4.2.1 利用目的の特定
4.4.2.2 適正な取得
4.4.2.3 特定の機微な個人情報の取得の制限
4.4.2.4 本人から直接書面によって取得する場合の措置
4.4.2.5 個人情報を4.4.2.4以外の方法によって取得した場合の措置
4.4.2.6 利用に関する措置
4.4.2.7 本人にアクセスする場合の措置
4.4.2.8 提供に関する措置
4.4.3 適正管理
4.4.3.1 正確性の確保
4.4.3.2 安全管理措置
4.4.3.3 従業者の監督
4.4.3.4 委託先の監督
4.4.4 個人情報に関する本人の権利
4.4.4.1 個人情報に関する権利
4.4.4.2 開示などの求めに応じる手続き
4.4.4.3 開示対象個人情報に関する周知など
4.4.4.4 開示対象個人情報の利用目的の通知
4.4.4.5 開示対象個人情報の開示
4.4.4.6 開示対象個人情報の訂正、追加又は削除
4.4.4.7 開示対象個人情報の利用又は、提供の拒否権
4.4.5 教育
4.5 個人情報保護マネジメントシステム文書
4.5.1 文書の範囲
4.5.2 文書管理
4.5.3 記録の管理
4.6 苦情及び相談
4.7 点検
4.7.1 運用の確認
4.7.2 内部監査
4.8 是正措置及び予防措置
4.9 事業者の代表者による見直し

3. 内部統制に関する既存の基準・ガイドラインの概要

内部統制に関する既存の基準・ガイドラインは、以下のように抽出・整理できる。

COBIT（IT Governance Institute）

企業・自治体といった組織のITガバナンスの指針として、米国の情報システムコントロール協会（ISACA）などが提唱するITガバナンスの実践規範のこと。フレームワークやガイドライン、成熟度モデル、ツールセットなどの一連の資料からなる。IT投資の評価、ITのリスクとコントロールの判断、システム監査の基準などに使われる。

SAS70（米国公認会計士協会）

米国監査基準第70号。米国公認会計士協会（AICPA）が定めた、アウトソーシングサービスなどの受託業務に関する内部統制を評価するための監査基準。受託業務を実施している企業は、SAS70に基づいて作成された報告書を提示すれば、組織の内部統制の仕組みが有効であることを委託者に認知されることが可能となる。

Web Trust（米国公認会計士協会）

WebTrustは、ECサイトのようなインターネットを利用した電子商取引を実施する事業者の内部統制について、実務慣行を基礎として定められたWebTrust原則および基準に準拠しているかを公認会計士が検証するサービス。主としてインターネットビジネスにおける利用者保護のための保証業務となっている 。

Sys Trust（米国公認会計士協会）

SysTrustは、電子商取引に限定されず、企業の情報システムの内部統制についてSysTrust原則および基準にもとづき特定の期間において有効に運用されているかを公認会計士が検証するサービス 。

4. SLAに関する既存の基準・ガイドラインの概要

SLAに関する既存の基準・ガイドラインは以下のように整理できる。

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（総務省）

電子自治体の構築にあたり、自治体間のシステム共同化、業務を民間へアウトソーシングする際必要となるプロジェクト、契約関係、SLAの内容について定めたガイドライン(2003年3月策定）

情報システムに係る政府調達へのSLA導入ガイドライン（経済産業省）

「情報システムに係る政府調達府省連絡会議」において決定された事項のうち、「調達管理の適正化」に関する具体例を示すため、SLAの重要性とその作成、発展のステップが盛り込まれたガイドライン。本ガイドラインは、「ITサービスの質を定量的に評価する尺度の確立」を目的としている。

電子自治体 基幹系SLA設定例（2006年　ASPIC Japan編 ASP・IDC活用による電子自治体アウトソーシング　実践の手引き）

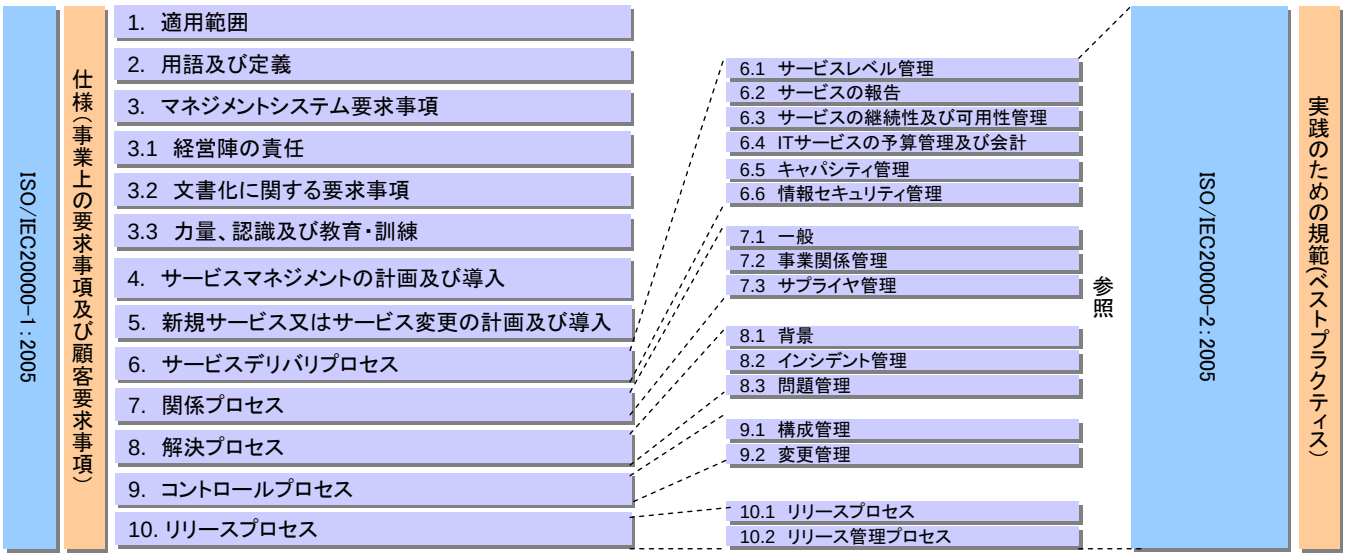
総務省にて策定された「公共ITにおけるアウトソーシングに関するガイドライン」の流れを受け、電子自治体構築におけるASP・IDCの有効活用を促進するために、それらの課題や進め方を解説した「ASP・IDC活用による電子自治体アウトソーシング　実践の手引」の基幹系SLA設定例として作成されたガイドライン

民間向けITシステムのSLAガイドライン　第3版（2006年　日本情報技術産業協会　JEITA）

既にガイドラインとして確立されていた、さまざまなガイドラインの流れを受け、JEITAは、SLA/SLM専門委員会を設置し、民間向けSLAの標準化活動を開始。その活動成果として、民間におけるSLAの共通指標を提示、ITサービスの利用者と供給者の間で適切なレベル選択が可能となることをめざしたガイドライン

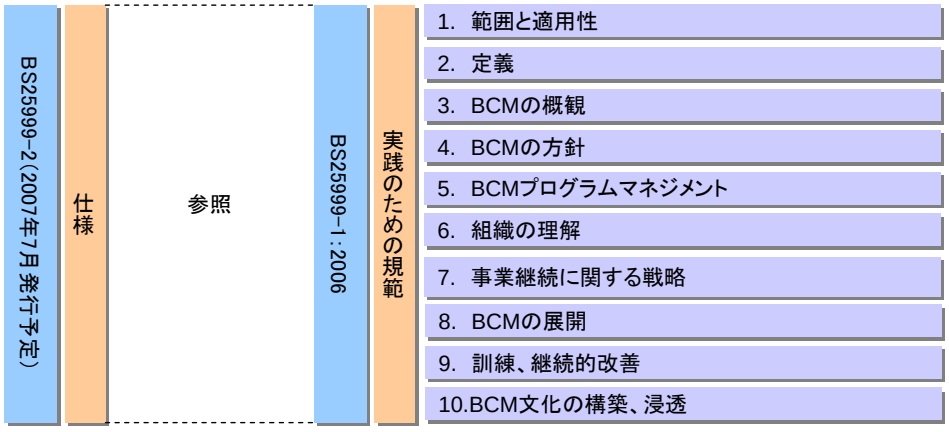
5. ITサービスに関する既存の基準・ガイドラインの構造

ITサービス分野に関する既存の基準・ガイドラインの構成・章立て及び関係は、以下のように整理できる。



6. 事業継続、信頼性に関する既存の基準・ガイドラインの構造

事業継続分野の基準・ガイドラインで、今後ISO化の可能性が高いBS25999-1の構成・章立て及びBS25999-2との関係は、以下のように整理できる。



事業継続・信頼性に関する既存の基準・ガイドラインの概要

事業継続・信頼性分野に関する既存の基準・ガイドラインの概要を以下に示す。

事業継続ガイドライン　第一版　（内閣府防災担当）

企業に対して事業継続の取組みの概要および効果を示し、防災のための社会的な意義や取引における重要性の増大、自社の受けるメリット等を踏まえて企業が自主的に判断するのを促すことを目的として策定されたガイドライン。ガイドラインには、具体的な取組みを簡易にチェックできるよう、「事業継続ガイドライン チェックリスト」が用意されている。(2005年8月策定）

事業継続計画策定ガイドライン　（経済産業省）

IT事故を想定した事業継続計画の策定手順や検討項目をわかりやすく解説することを念頭に策定されたガイドライン。内容は、①事業継続策定に際しての基本的な考え方、②策定時に考慮すべき総論的事項、③事業継続計画策定に当たっての具体的検討事項、④IT事故を想定したケーススタディ及び⑤参考資料としてベストプラクティス事例等が盛り込まれている。（2005年8月策定）

中小企業BCP策定運用指針　（中小企業庁）

自然災害や大火災等の緊急事態において事業中断を最短にとどめ被害を最小化するための企業の危機管理の新手法として、主に欧米で発達し普及しているBCPの策定と運用のノウハウを我が国の中小企業向けに初めてわかりやすく解説した指針

金融機関等におけるコンティンジェンシープラン策定のための手引書（金融情報システムセンター）

大規模な自然災害や不慮の事故等といった不測の事態が発生した場合にも、業務の継続を図る手段を講じるため、あらかじめ各金融機関等がコンティンジェンシープラン(災害時の緊急時対応計画)を作成する際の手引書

情報通信ネットワーク安全・信頼性基準（昭和62年郵政省告示第73号）

情報通信の健全な発展とその安全・信頼性の向上を図ることを目的として定められたガイドライン。登録の対象となる情報通信ネットワークは、第二種電気通信事業の用に供する情報通信ネットワークや電子計算機を用いて計算、検索その他情報処理を行うオンライン情報処理業のネットワークなど。

参考資料　Ⅱ
（その他）

資料Ⅱ－１

研究会構成員一覧

（敬称略、五十音順）

	青木　　英司	日本電気㈱ 公共ソリューション事業部 事業推進部長
	今田　　正実	㈱富士通ビジネスシステム アウトソーシングサービス統括部 統括部長代理 兼 ＩＴアウトソーシングサービス部長
	岩下　　安男	㈱大阪エクセレント・アイ・ディ・シー 代表取締役社長
	上原　　稲一	沖縄電力㈱ 取締役 ＩＴ推進本部 部長
	及川　　喜之	㈱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
	小倉　　博行	三菱電機㈱ インフォメーションシステム事業推進本部 システム統括部 システム第一部 主席技師長
	木村　　隆司	ブレイン㈱ 執行役員 セールス＆マーケティング
	小林　慎太郎	㈱野村総合研究所 社会産業コンサルティング部 上級コンサルタント
【座　長】	佐々木　良一	東京電機大学　教授
	津田　　邦和	特定非営利活動法人ＡＳＰインダストリ・コンソーシアム 常務理事技術部会長
【座長代理】	中尾　　康二	ＫＤＤＩ㈱ 運用統括本部 情報セキュリティフェロー
	西山　　敏雄	ＮＴＴコミュニケーションズ㈱ ブロードバンドＩＰ事業部 ＩＰテクノロジー部長
	花戸　　俊介	トライコーン㈱ 取締役
	林　　敏	㈱ミロク情報サービス 取締役
【座長代理】	藤本　　正代	情報セキュリティ大学院大学 客員准教授
	松橋　　義樹	㈱サンスイ インフラソリューション部 部長
	宮坂　　肇	㈱ＮＴＴデータ 公共ビジネス推進部 技術戦略部 セキュリティ技術推進担当部長

資料Ⅱ－２

研究会開催要綱

1 背景・目的

ブロードバンド化の進展により、国民生活や社会経済活動における ICT への依存度が高まる中で、ネットワークを通じてオンデマンドにアプリケーションソフト等の機能として提供する新たな ICT サービス（ASP（Application Service Provider）・SaaS（Software as a Service）等）の利用が進み、昨今は“Web2.0”といった新たな概念が生まれている。

企業等における ASP・SaaS の利用においては、システムの保守・運用・管理にかかる負担が軽減される等のメリットがある一方で、ASP・SaaS 事業者及びその関係企業において、企業等の膨大な機密情報・顧客情報が集積されることとなるため、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となっている。

本研究会は、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 が企業の生産性向上の健全な基盤となるよう、当該サービスの実態、セキュリティ対策の現状、今後の進展等を把握し、当該サービスの提供事業者が講ずべき情報セキュリティ対策を事業内容等に沿って検討する。

2 名称

本会合は、「ASP・SaaS の情報セキュリティ対策に関する研究会」（以下「研究会」という。）と称する。

3 主な検討事項

（1） ASP・SaaS における情報セキュリティ対策の現状及び課題の把握について

（2） ASP・SaaS 事業者がサービスを提供するにあたって実施すべき情報セキュリティ対策について 等

4 構成員

別紙のとおり

5 運営

（1） 本研究会は、政策統括官（情報通信担当）の研究会とする。

（2） 本研究会には、座長及び座長代理を置く。

（3） 座長は、構成員の互選により定め、座長代理は座長が指名する。

（4） 座長は、本研究会を招集し、主宰する。

（5） 座長代理は、座長を補佐し、座長不在のときには、座長に代わって、本研究会を招集し、主宰する。

（6） 座長は、必要に応じ、関係者等の出席を求め、意見を聞くことができる。

（7） 座長は、上記の他、本会の運営に必要な事項を定める。

6　庶務

本研究会の庶務は、情報通信政策局情報セキュリティ対策室が行う。

7　開催期間

平成19年6月から平成20年1月頃を目処に計5回程度の開催を予定。

資料Ⅱ－３

研究会開催状況

日程	検討内容
第1回 平成19年6月21日	○研究会の目的及び検討スケジュールについて ○ASP・SaaS の現状について 【構成員プレゼンテーション】 ・津田構成員（特定非営利活動法人ASPICジャパン） ・今田構成員（㈱富士通ビジネスシステム） ・及川構成員（㈱セールスフォースドットコム）
第2回 平成19年8月8日	○ASP・SaaS における情報セキュリティ対策の現状・課題 【構成員プレゼンテーション】 ・宮坂構成員（㈱NTTデータ） ・花戸構成員（トライコーン㈱） ○ASP・SaaS の情報セキュリティ対策に関連する基準・ガイドライン 等
第3回 平成19年10月17日	○ASP・SaaS における情報セキュリティ対策の現状・課題 【構成員プレゼンテーション】 ・小倉構成員（三菱電機㈱） ・木村構成員（ブレイン㈱） ○ASP・SaaS における情報セキュリティ対策ガイドライン（叩き台）の検討
第4回 平成19年12月18日	○ASP・SaaS における情報セキュリティ対策ガイドライン（案）の確認 ○ASP・SaaS の情報セキュリティ対策に関する研究会報告書（案）の確認
報告書案等に対する意見募集 平成19年12月19日～平成20年1月18日	
第5回（最終会合） 平成20年1月29日	○報告書案等に対する意見募集の結果について ○情報セキュリティ対策ガイドライン及び報告書の最終とりまとめ
報告書案等に対する意見募集の結果及び報告書等の公表 平成20年1月30日	

報告書案等に関する意見募集の結果及び研究会における考え方

１　実施期間

平成１９年１２月１９日から平成２０年１月１８日まで

２　意見件数

計８件

３　意見提出者一覧

（受付順、敬称略）

番号	意見提出日※	意見提出者
1	平成20年1月4日	個　人
2	平成20年1月17日	日本ユニシス株式会社
3	平成20年1月17日	社団法人情報サービス産業協会
4	平成20年1月18日	株式会社ラック
5	平成20年1月18日	社団法人日本薬剤師会
6	平成20年1月18日	社団法人山形県情報産業協会
7	平成20年1月18日	株式会社パイプドビッツ
8	平成20年1月18日	ソフトバンクテレコム株式会社

※意見提出日は、総務省に提出された日（受付日）を記載しております。

４　意見に対する考え方

別表参照

（別　表）

対象	該当箇所	意　　見※	研究会における考え方
全般	－	表題の「ASP・SaaS」を「ソフト利用サービス（ASP・SaaS）」と改めて、中小企業従業員全てに分かりやすくすべき。まず、中小企業従業員全てが取り付きやすくする必要があり、ASP・SaaS は「ソフト利用サービス」で足りる。 【個人】	ASP やSaaS という表現は､「成長力加速プログラム」（平成 19 年 4 月 25 日 経済財政諮問会議）や「ICT 改革促進プログラム」（平成 19 年 4 月 20 日 総務省）等にも使用されており、一般に認知されているものと認識しております。また、ガイドラインⅠ．２項において、その定義を明示しているところでもあり、原案のままで問題ないと考えます。
	－	経済産業省「SaaS 向け SLA ガイドライン（案）」との関係はどのようになっているのか。 【社団法人情報サービス産業協会】 【社団法人山形県情報産業協会】	本ガイドラインは、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することを目指して策定したものであり、本ガイドラインをそのまま利用することで、ASP・SaaS 事業者が比較的簡単に適切な情報セキュリティ対策を実施できるように構成しています。
	－	総務省が平成１９年１１月２７日に公表した「ASP・SaaS の安全・信頼性開示指針」の報道発表資料において、「認定を行う仕組み」についての言及があるが、ガイドラインを業界内に普及することが重要であり、これ以上の認定制度は必要ないというのが業界の基本認識である。むしろ、事業者の負担を考えれば、既存の認定制度の整理統合を視野に入れた政策立案こそ重要と考える。 【社団法人情報サービス産業協会】	ご意見の内容は、本件意見募集の対象外です。
	－	SaaS のような新たなサービスの健全な発展のためには、まず提供サービスの内容をユーザが理解し、その上でサービスレベルについて利用者、供給者が適切な取引関係を構築できるよう環境整備を図る必要があり、利用者の安全・安心を確保するためのツールとして、今回のガイドラインは有益である。 【社団法人情報サービス産業協会】 SaaS の可能性について早期に注目し、SaaS 提供企業と利用者との紛争を未然に防ぐことを目的に、総務省において「ASP・SaaS の情報セキュリティ対策に関する研究会」が主催され、本ガイドライン案の策定および研究会報告書の公開に至ったことについて、山形県内の情報システム提供側の業界団体としてその趣旨に賛同する。 【社団法人山形県情報産業協会】	本案を支持するご意見として承ります。
	－	SaaS を全くの新技術ととらえ、日本発の体系的な SaaS 時代のセキュリティ人材育成プログラムなどの国家プロジェクトを先導し、世界標準を目指すような戦略を打ち出すことを期待する。 また、SaaS ビジネスにおいて地方の独立系 IT 企業が	ご意見の内容は、本件意見募集の対象外です。

		担うべき社会的役割、中央と地方が担う情報産業の将来展望について、今後ともよりいっそう踏み込んだ議論の場を設けるべく、情報開示およびパブリックコメントの場を継続することを希望する。 【社団法人山形県情報産業協会】	
	―	本ガイドラインに準拠したとしても、ASP･SaaS 事業者間で同等のセキュリティレベルが確保されていることは保証の限りでないため、事業者同士が民間の中立な協議会的組織を通じてセキュリティレベルを評価しあう仕組みが必要。 【ソフトバンクテレコム株式会社】	報告書第４章４．２．１【１】項において、ASP・SaaS 業界におけるガイドラインの積極的な活用を今後の課題として挙げており、ご意見にある ASP・SaaS 事業者同士のセキュリティレベルの相互評価のような仕組みについても、ガイドライン活用策のひとつと考え、ASP・SaaS 業界内で適宜検討されることを期待します。
	―	システム構成要素の区分も継続的な見直しの対象となるべき。具体例を挙げるならば、システムインフラ(PaaS: Platform As a Service)とアプリケーション(Software As a Service)を分離して指針を定めるほうがASP・SaaS ユーザの立場でセキュリティ対策状況を理解することが容易となる面もある。 【ソフトバンクテレコム株式会社】	報告書第４章４．２．１【２】項において、ASP・SaaS の利用環境の変化に対応したガイドラインの見直し・改善の必要性を今後の課題として挙げており、ご意見の趣旨は踏まえているものと認識しております。
報告書	２．１	ASP・SaaS 事業者の業態は、大企業を含めて評価すべき。「ASP・SaaS 業界は、中小事業者を中心に構成されていること」「セキュリティ対策の必要性」が強調され、中小企業者が不安を感ずる惧れがある。現に、情	報告書第２章２．１．３項の ASP・SaaS 事業者に対するインタビュー調査では、中小企業だけではなく大企業の ASP・SaaS 事業者も含めて評価しております。

		報通信大企業系のソフトウェア会社や基幹電気通信事業者が、ほとんど全て ASP・SaaS への参入に、既に着手し、または参入を予告しているところ。 【個人】	
	３．１	「新興 ASP・SaaS 事業者向けの支援策、助成制度」項目を追加。 知識提供だけでベンチャーが ASP・SaaS ビジネス分野を牽引できるとは考えられず、保護政策としての助成制度も同時に検討いただくことを期待する。 【社団法人山形県情報産業協会】	本研究会の検討事項は、ASP・SaaS サービス事業者が取り組むべき情報セキュリティ対策であるため、ご指摘の内容は報告書になじまないものと考えますが、ご意見として参考とさせていただきます。
	３．２．３	「医療・介護・福祉」のサービス種別について、現在示されているサービスの定義は、電子的作成が認められていない処方箋に関するものが列挙されるなど、医療関係者から見た場合、一部誤解を招く表現も含まれていることも踏まえ、提供サービスの実態を踏まえた記載に改めることが望ましいと考える。 また、医療分野における個人情報は、とりわけ秘匿性の高い情報であることから、医療・介護・福祉サービスの機密性は全て「高」に分類されることが当然と考えられる。 可用性についても、医療・介護・福祉事業の業務プロセスに直接関係するサービスは、一般において連動して稼動していることからも、常に稼動している必要がある	ご指摘のとおり修文することとします。

<table>
<tr><td></td><td></td><td>と考えられる。
　したがって、「医療・介護・福祉事業特化型 ASP（電子カルテ、レセプト）」「医療・介護・福祉事業特化型 ASP（診療予約、介護業務支援）」「医療・介護・福祉事業特化型 ASP（処方箋サービス）」を統一した上で、下図のように修正すべき。

<table>
<tr><th rowspan="2">サービス種別</th><th rowspan="2">サービスの定義</th><th colspan="3">機密性</th><th colspan="4">可用性</th></tr>
<tr><th>高</th><th>低</th><th>理由</th><th>高</th><th>中</th><th>低</th><th>理由</th></tr>
<tr><td>医療・介護・福祉</td><td>診療予約・介護業務支援等、医療・介護・福祉事業の業務プロセスを支援するサービス</td><td>○</td><td></td><td>一般個人情報の保持</td><td>○</td><td></td><td></td><td>常に稼動の必要あり</td></tr>
</table>

【社団法人日本薬剤師会】</td><td></td></tr>
<tr><td>ガイド</td><td></td><td>対策項目・ベストプラクティスの提示に留め、評価項目は削除すべき。ガイドラインの発行者が総務省であることにより、実質的な拘束力が生ずる可能性があるにもかかわらず、評価項目が具体的かつかなり高いレベルとなっているため、中小・ベンチャー企業がどこまで本ガイドラインに準拠できるか疑問がのこる。また、サービス提供価格の高騰に繋がることが危惧される。
　さらに、評価項目・対策参照値のような基準を定めるならば、タイムリーかつ継続的な見直しが必要不可欠であり、こうした役割は民間の中立的な協議会的組織に委ね、政府は促進・支援する立場に身をおくべき。
【ソフトバンクテレコム株式会社】</td><td>［前段部分］本ガイドラインは、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策定しており、その十分な活用を促すためには、評価項目と対策参照値の設定により、対策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を示すことが望ましいと考えます。
　また、本ガイドラインで示している対策実施レベルについては、中小 ASP・SaaS 事業者を含む研究会構成員による議論に基づいており、実態から乖離したものとはなっていないと考えられ、ご指摘のご懸念はあたらないものと考えます。
　なお、本ガイドラインは本研究会において取りまとめるものです。
［後段部分］報告書第４章４．２．１【２】項に示しているとおり、ASP・SaaS 業界においてガイドラインの継続的な見直し・改善が実施される体制の構築を期待するものであり、ご意見の趣旨は踏まえているものと認識しております。</td></tr>
<tr><td>ライン</td><td></td><td>「本ガイドラインは JIS Q 27001(ISO/IEC27001)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にしている。」とあるが、「参考」の意味するところが曖昧であるため、より明確に記述していただきたい。</td><td>　本ガイドラインの検討にあたっての、既存の基準・規範等の参考の仕方については、報告書第３章３．２項に記載したとおりです。
　また、本ガイドラインは、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</td></tr>
</table>

		【社団法人山形県情報産業協会】 本ガイドラインと、JIS Q 27001（ISO/IEC 27001）及び JIS Q 20000（ISO/IEC 20000）の関連性について、当該認証を取得している事業者にとって本ガイドラインに適合することの有効性を含め、見解をお示しいただきたい。 【株式会社パイプドビッツ】	策を実施するための指針となるように、ASP・SaaS に特化された具体的な対策集として構成されています。情報セキュリティに関する認証等を取得している ASP・SaaS 事業者にとっても、実施すべき情報セキュリティ対策の検討において参考になるものと考えます。
	Ⅰ．７	機密性への要求の「低」の区分けはなくし、「高」又は「中」とすべき。「低」を残すのであれば、情報セキュリティが軽視されないような注意事項の記述を追加すべき。 【日本ユニシス株式会社】	ガイドラインⅠ．７．１項に示す「機密性への要求の高低に関する考え方」のとおり、「高」「低」という表現は、一定の条件に合致するかどうかの相対的な差を示す“見出し”として用いているものであり、「低」が絶対的なセキュリティ要求レベルの低さを示すものではありません。 しかしながら、ご指摘のとおり、当該表現が本ガイドライン参照者における情報セキュリティ対策の軽視に繋がる可能性も否定できないことから、該当部分に上記の趣旨の注記を追加することとします。
	Ⅱ	「Ⅱ 組織・運用編」の全体の構成の在り方について、「基本方針」「組織」「連携 ASP・SaaS 事業者」「情報資産」「従業員」「インシデント」「コンプライアンス」「サービスサポート」という８つの節構成にて記載があるが、その根拠について説明を入れるべき。 【日本ユニシス株式会社】	ガイドライン「Ⅱ組織・運用編」における情報セキュリティ対策の導出過程は、報告書第３章３．２．２項に記載しております。具体的には、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た上で、ASP・SaaS サービスのステークホルダの構成を考慮し、中小事業者にとっても優先的に取り組むべき対策に重点を置いた導出を行いました。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た結果、8 つの節から構成される対策集としてとりまとめるに至っております。
	Ⅱ．２．２．１	ベストプラクティスに「iv ASP・SaaS サービスの提供にあたり、海外にデータセンタがある場合等、海外法が～」とあるが、「Ⅱ．７ コンプライアンス」に移したほうが自然ではないか。 【日本ユニシス株式会社】	ご意見を踏まえ、対策項目「Ⅱ．７．１．１」のベストプラクティスに移すこととします。
	Ⅱ．７	海外法への対応事例として、以下をベストプラクティスに追記する価値があるか否か検討をお願いする。 ■暗号化ソフトウェアの国外持ち出し時の注意事項として下記を追記。 「海外出張に当たってモバイル PC 等を帯同する場合、暗号化ソフトウェアの取扱に関して関連部署に問い合わせ、指示を仰ぐ必要がある。抵触した場合、入国審査時にモバイル PC が没収される恐れがあるため、暗号化ソフトを削除する。」 【日本ユニシス株式会社】	ご指摘の事項は、ASP・SaaS サービスの情報セキュリティ対策に直接関係する内容ではないため、本ガイドラインに追記する必要はないと考えますが、ご意見として参考とさせていただきます。
	Ⅱ．８．１	ASP・SaaS ビジネスの成長段階において発生する事業者の撤退など予期せぬサービス停止について、ユーザの被害を最小限にとどめるため、ASP・SaaS 運用およびサービスの永続性に関する指標を事業者が明示する	ご指摘の事項は、ASP・SaaS サービスの情報セキュリティ対策に直接関係する内容ではないため、本ガイドラインに追記する必要はないと考えますが、ご意見として参考とさせていただきます。

		ことを提案する。 【社団法人山形県情報産業協会】	
	Ⅱ．８．２	「利用者が負うべき責任」項目を追加。 インターネットに公開されている ASP・SaaS においては、正規ユーザとそれ以外に峻別すると、システムのセキュリティ対策のレベル、コストが大きく異なる。マルチテナントのシステムに対して、正規ユーザが不正に他社の情報を入手することを目的に行う攻撃に対しては、システム対策上のコストが過度に増大する。事前に ASP・SaaS 事業者と利用者が負うべき責任を明確にすることで、ASP・SaaS 事業者が追うべきリスクを限定すること。 また、利用者の、①インターネット接続は帯域保証されていないこと、利用者が管理している②PC の性能やインストール済みソフトウェアは千差万別であること、このことを ASP・SaaS 事業者は利用者に告知し、ASP・SaaS 事業者の過失以外にも ASP・SaaS サービスが停止する可能性のあることを、利用者が負うべき責任として明示すること。 【社団法人山形県情報産業協会】	本ガイドラインは、ご指摘のような正規ユーザからの攻撃についても視野に入れたものとなっていると考えます。また、本ガイドラインのⅠ．３項に記載したとおり、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、本ガイドラインの対象外としています。これらの事項の取り扱いについては、ASP・SaaS 事業者と利用者との間の個々の取り決めによると考えます。
	Ⅱ．８．３	「利用者向け ASP・SaaS 知識取得支援」項目を追加。 専門知識が不足している利用者と ASP・SaaS 事業者の契約行為においては、利用者に不利な状況が発生しやすい。これを防止する目的で、対等な交渉を成立させるための「利用者向け ASP・SaaS 知識修得の支援」を行う責任が、ASP・SaaS 事業者にあることを明示すること。 利用者にとって ASP・SaaS を利用する上での必要となる知識を、利用者が理解できる用語で説明する「ASP・SaaS ユーザ向け利用のガイドライン」の整備・充実を求める。 【社団法人山形県情報産業協会】	ご指摘の事項は、ASP・SaaS サービスの情報セキュリティ対策に直接関係する内容ではないため、本ガイドラインに追記する必要はないと考えますが、ご意見として参考とさせていただきます。
	Ⅲ	ASP・SaaS では、まずアプリケーションがセキュアであることが必要。アプリケーション開発プロセスや完成したアプリケーションのセキュリティ検査についても記述することを要望する。 【株式会社ラック】	ご指摘を踏まえ、対策項目「Ⅲ．２．１．４」のベストプラクティスに、「ASP・SaaS サービスの提供に用いるアプリケーションについては、開発段階からぜい弱性診断を行うこと等により、導入前にあらかじめぜい弱性対策を実施しておくことが望ましい。」と追記することとします。
	Ⅲ．２．１．３	ベストプラクティスにおいて、取得することが望ましい情報の例示にデータベースのテーブルに格納された情報へのアクセスが想定されていない。以下のような例示を加えることを要望する。 m)データベースへのアクセスの場合は、アクセスされたテーブル及び SQL 文 【株式会社ラック】	データベースへのアクセスについては、ベストプラクティス「e) データ及び他の情報資産へのアクセスの～」において記載されているものと考えます。
	Ⅲ．２．１．３	ログの取得と保存期間に関する指針でありながら、唐	評価項目ｃ．は、ログの連続性の観点から設定され

		突に評価項目ｃ.には「スタンバイ機による運転再開」と記載されており、意図が不明瞭である。 【株式会社パイプドビッツ】	ているものであり、対策項目「Ⅲ．２．１．３」を実施する際の指標として適当と考えます。しかしながら、意図が伝わりにくいというご指摘を踏まえ、「Ⅲ．２．１．３」のベストプラクティスに、「システム障害などによるログの欠損をできる限りを少なくするために、スタンバイ機等を用いてログサーバの運転を迅速に再開できる状態にしておくことが望ましい。」と追記することとします。
	Ⅲ．２．１．４	「定期的にぜい弱性診断を行い」とあるが、アプリケーションのリリース時及び改版時は新たなぜい弱性が作られるケースが多いため、パターンを問わず、アプリケーション開発業者以外の第三者による脆弱性診断を実施すべきであることを明示することを要望する。 【株式会社ラック】	アプリケーション導入前の脆弱性診断については、前記ご意見を踏まえ、ベストプラクティスに追記することとしています。また、評価項目 b.及び c.において、外部委託によるぜい弱性診断も含む旨記載しております。 ぜい弱性診断を行うタイミング及び実施する機関等については、各 ASP・SaaS 事業者において判断されるべきものと考えます。
	Ⅲ．２．２．２	多くの ASP・SaaS では認証情報として、ユーザ ID とパスワードが利用されていると思われる。利用者は同一の ID・パスワードを他のサイトの認証情報として設定していることは少なくなく、実際に過去の不正アクセスや情報漏えい事件において、他のサイトで悪用されたケースも存在する。したがって、パスワードに関しては、パスワード文字列ではなく、ハッシュ値を保存しなくてはならない旨、明示することを要望します。 【株式会社ラック】	ご指摘の事項については、対策項目「Ⅲ．３．１．３」における ID・パスワードの運用管理方法に関するものと考え、「Ⅲ．３．１．３」のベストプラクティスに、「ID･パスワード等の認証情報は、文字列ではなくハッシュ値 を保存することが望ましい。」と追記することとします。
	Ⅲ．３．１．５	「不正な通過パケットを自動的に発見する措置（IDS の導入等）を講じること。」との記載があるが、今般販売されている商用の不正な通過パケットの自動発見機器は IPS に相当する能力をもつ機器が主流であるため、推奨項目ではあるが、「不正な通過パケットを自動的に発見、もしくは遮断する措置（IPS の導入等）を講じること。」として IPS を対象機器として加えることを検討すべき。 【株式会社ラック】	ご指摘を踏まえ、「不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS／IPS の導入等）を講じること。」と修文することとします。
	Ⅲ．５．２．１	「運用管理端末におけるログイン・ログアウト、特定プログラムの実行、データベース接続などの重要操作のロギング」を追加することを要望する。 【株式会社ラック】	ご指摘を踏まえ、「Ⅲ．５．２．１」のベストプラクティスに、「運用管理端末において、従業員等が行うログイン・ログアウト、特定プログラムの実行、データベース接続などの重要操作等について、操作ログを取得し、保存することが望ましい。」と追記することとします。

※ご意見は要約を記載しています。