資料3-4

ASP・SaaSにおける情報セキュリティ対策の動向
（インタビュー調査より）

ASP・SaaSの情報セキュリティ対策に関する研究会
事務局

2007年10月17日

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。

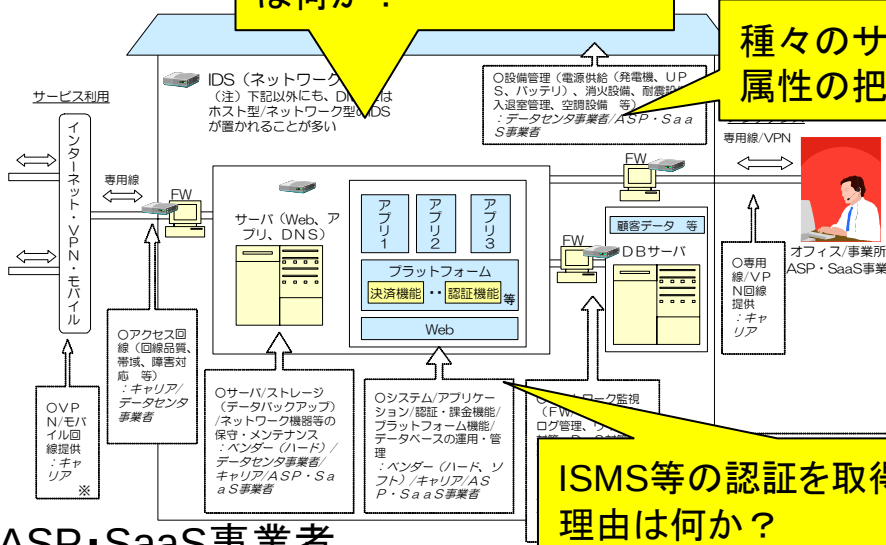
ユーザの
SLA要求の
実状は？

どのような属性の企業が現在
ユーザとなっているか？

ISMS等の認証を取得していないことに
対するユーザ側の対応の実状は？

ASP・SaaSに特化した情
報セキュリティ上の課題
は何か？

種々のサービス基本
属性の把握



ISMS等の認証を取得していない
理由は何か？
これが原因でどのような問題が生
じうると自ら考えるか？

ASP・SaaS事業者
（事業・組織規模や成熟度が
十分でない）

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）

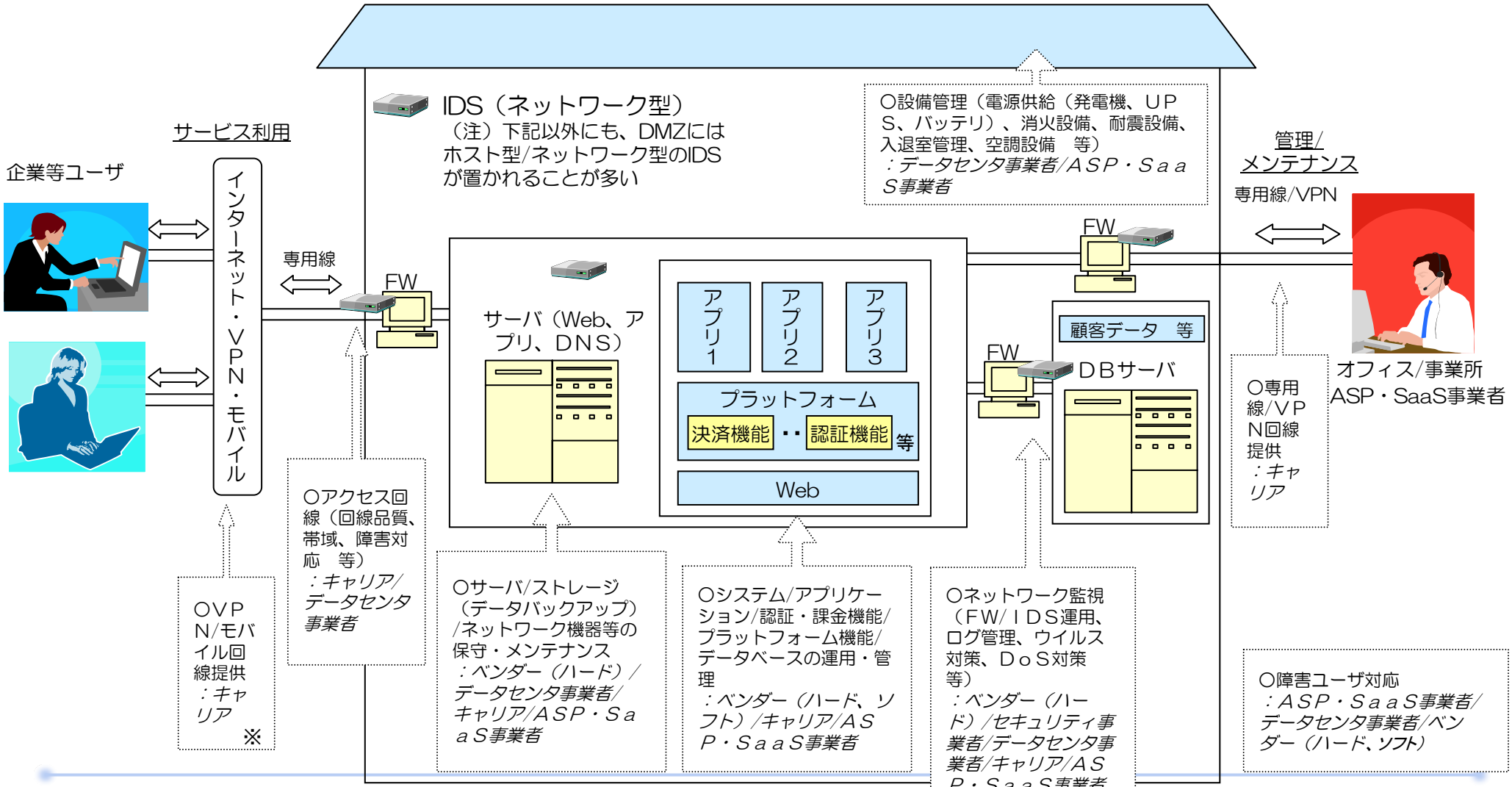
（参考）調査対象としたASP・SaaS事業者のシステムアーキテクチャと運用

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	ー
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

（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

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