資料５－２

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（案）

ASP・SaaS の情報セキュリティ対策に関する研究会
事務局

2008 年 1 月 29 日

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	ご意見の内容は、本件意見募集の対象外です。

		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】	
	―	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。

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。

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
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

【社団法人日本薬剤師会】

ガイド		対策項目・ベストプラクティスの提示に留め、評価項	［前段部分］本ガイドラインは、ASP・SaaS 事業者が

ライン		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】	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。
		「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。	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

		【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	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

		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】	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	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。

		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】	
	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。