

ASP・SaaSの安全・信頼性に係る
情報開示指針に関する検討結果（案）

2007年11月20日

ASPIC ジャパン

(ASP インダストリ・コンソーシアム・ジャパン)

目 次

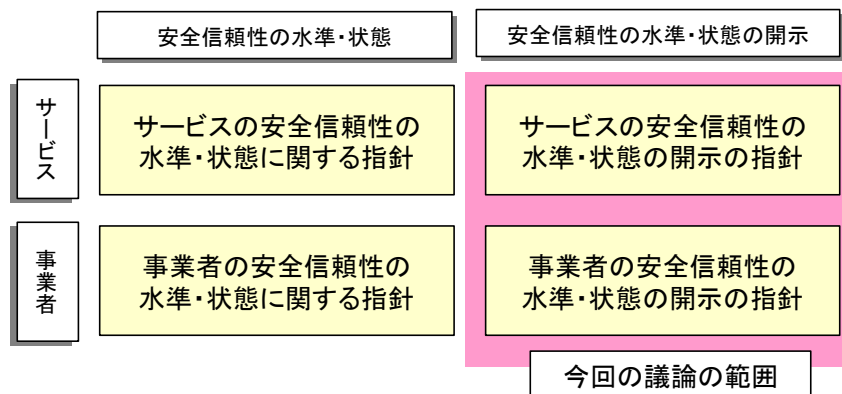
1. 検討の目的
2. 業界レベルでのガイドライン策定事例の整理
3. 電気通信事業法改正と消費者保護ルール制定の事例
4. 安全・信頼性 WG 等での検討内容の整理
5. ASP 事業者・サービスの情報開示項目の検討

1. 検討の目的

中小企業をはじめとするユーザは、ASP サービスを安心かつ継続的に活用できることを、ASP・SaaS 事業者に対し望んでいる。しかしながら、現状では ASP・SaaS 事業者からユーザへの十分な情報の提供（開示）がないために、ASP・SaaS 市場は過小な市場規模になっていると考えられる。その対応として、ASP・SaaS 事業者はユーザに対し、ユーザの適切な事業者及びサービスの選定に必要な、十分な情報の提供（開示）を行うことが求められる。

上記の考えに基づき、ASP・SaaS 事業者及びサービスの安全信頼性の水準・状態についての情報開示のための指針を策定する。なお、安全信頼性開示指針の検討の範囲は、下図のとおりとする。

図表 ASP・SaaS 安全信頼性開示指針の検討範囲



2. 業界レベルでのガイドライン策定事例の整理

既存のガイドライン策定事例中、今回の議論の対象となっている「安全信頼性の状態の開示」について言及しているものは以下の通りであった。

金融業を中心としたディスクロージャー基準では、財務情報を中心として、業務情報及び社内におけるリスク管理に関する情報の開示を求めている。また、各種業界において制定されているサービス提供に関するガイドラインにおいては、具体的な開示項目の有無において差はあるものの、開示規定が設けられているものがある。

図表 情報開示を規定しているガイドラインの項目例 1

日本損害保険協会 2007年度 ディスクロージャー基準	生命保険協会 ディスクロージャー開示基準	日本商品先物取引協会 会員(開示企業)の情報開示項目
1. 保険会社の概況及び組織 2. 保険会社の主要な業務の内容 3. 保険会社の主要な業務に関する事項 4. 保険会社の運営 5. 直近の2事業年度(特に指定のあるものを除く)における財産の状況 6. 保険会社及びその子会社等の概況 7. 保険会社及びその子会社等の主要な業務 8. 保険会社及びその子会社等の直近の2連結会計年度における財産の状況 9. 設備の状況	I. 保険会社の概況及び組織 II. 保険会社の主要な業務の内容 III. 直近事業年度における事業の概況 IV. 直近5事業年度における主要な業務の状況を 示す指標 V. 財産の状況 VI. 業務の状況を示す指標等 VII. 保険会社の運営 VIII. 特別勘定に関する指標等 IX. 信託業務に関する指標 X. 保険会社及びその子会社等の状況	会社の概況 ・会社名等 ・会社の沿革 ・会社の目的 ・事業の内容 ・営業所の状況 ・財務の概要 ・発行済株式総数 ・主要株主名 ・役員の状況 ・従業員の状況 営業の状況 ・営業方針 ・当社および当業界を取り巻く環境 ・営業の経過および成果 ・対処すべき課題 ・受託業務管理規則 ・外務員の登録状況 ・委託者数 ・苦情・紛争に関する事項 ・訴訟に関する事項 経理の状況 ・貸借対照表 ・損益計算書 ・重要な会計方針 ・注記事項 ・利益金処分計算書 ・監査に関する事項 ・財務比率

図表 情報開示を規定しているガイドラインの項目例 2

タイムビジネスに係る指針(総務省)	情報通信ネットワーク安全・信頼性基準(総務省)
<p>1. 目的</p> <p>2. タイムビジネスのイメージ</p> <p>3. タイムビジネスの必要性</p> <p>4. 用語</p> <p>(1) 時刻配信業務</p> <p>(2) 時刻認証業務</p> <p>(3) タイムビジネス</p> <p>(4) 検証者</p> <p>(5) 標準時</p> <p>5. タイムビジネスに求められる事項</p> <p>(1) 時刻配信業務</p> <p>ア) 省略</p> <p>イ) 省略</p> <p>ウ) 時刻監査を行う場合には、配信先の設備を特定してその時刻精度を定期的に計測するとともに、その結果を当該設備に送信又は時刻監査を求めた者に報告すること。</p> <p>エ) 時刻配信業務に関する監査を受けること。なお、時刻配信業務では、時刻監査を求めた者その他の者の求めに応じ、時刻情報の配信元とその維持精度に係る情報を提示できることが望ましい。</p> <p>(2) 時刻認証業務</p> <p>ア) 省略</p> <p>イ) 省略</p> <p>ウ) 省略</p> <p>エ) 省略</p> <p>オ) 省略</p> <p>カ) 省略</p> <p>キ) 省略</p> <p>ク) 検証者に対して、次の事項が理解できるように情報を適切に提供すること。・時刻認証業務の概要(上記キ)に記載した説明事項の概要)・電子データとそれに係るタイムスタンプ及び検証必要情報、並びに検証結果に係る情報の適切な保存</p> <p>ケ) 時刻認証業務に関する監査を受けること。また、時刻認証業務を行う事業者は、当該業務で付与したタイムスタンプの有効性を保証する期間内において業務を継続することが困難となった場合には、速やかにすべての利用者に対して、その旨を通知するとともに、当該タイムスタンプの有効性が確保できるように努めること。なお、時刻認証業務では、利用者又は検証者の求めに応じ、時刻情報の配信元とタイムスタンプに用いた時刻情報の維持精度に係る情報を提示できることが望ましい。</p>	<p>情報通信ネットワーク安全・信頼性基準(総務省)</p> <p>設備等基準</p> <p>設備基準</p> <p>一般基準(13項目、53対策)</p> <p>屋外設備(15項目、20対策)</p> <p>屋内設備(7項目、12対策)</p> <p>電源設備(7項目、14対策)</p> <p>環境基準</p> <p>センターの建築物(4項目、11対策)</p> <p>通信機械室など(6項目、21対策)</p> <p>空調調和設備(8項目、15対策)</p> <p>管理基準</p> <p>ネットワーク設計管理(4項目、6対策)</p> <p>ネットワーク施工管理(5項目、6対策)</p> <p>ネットワーク保全・運用管理(9項目、14対策)</p> <p>設備の更改・移転管理(2項目、2対策)</p> <p>情報セキュリティ管理(7項目、8対策)</p> <p>データ管理(5項目、7対策)</p> <p>環境管理(2項目、2対策)</p> <p>防犯管理(6項目、6対策)</p> <p>非常事態への対応(2項目、7対策)</p> <p>教育・訓練(2項目、8対策)</p> <p>現状の調査・分析及び改善(4項目、5対策)</p> <p>安全・信頼性の確保等の情報公開(2項目、2対策)</p>

図表 情報開示を規定しているガイドラインの項目例 3

民間向けITシステムのSLAガイドライン	葬祭サービスガイドライン(全日本葬祭業協同組合連合会)
<p>ITサービス評価項目</p> <p>セキュリティサービス サービス全体/情報提供サービス/セキュリティ診断サービス/IDSサービス/ 改竄検知サービス/ウイルス対策サービス/ファイアウォールサービス</p> <p>保守サービス HW障害対策/SW障害対策</p> <p>運用サービス 障害対応サービス/運転対応サービス/サポート対応サービス</p> <p>サポートデスクサービス ヘルプデスクサービス</p> <p>アプリケーション運用サービス 定型業務/非定型業務/業務共通</p> <p>ネットワークサービス 回線通信/LAN通信/運用管理/障害管理</p> <p>ITプロセスマネジメント評価項目</p> <p>アプリケーション管理 サービスレベル管理/キャパシティ管理(資源管理)/セキュリティ管理/ リリース管理/構成管理/ITサービス継続性管理</p> <p>変更管理 サービスレベル管理/構成管理/リリース管理/変更管理/ キャパシティ管理(資源管理)/セキュリティ管理/可用性管理(稼働管理)/問題管理/ インシデント管理(発生事象管理)/ITサービス継続性管理/問題管理/インシデント管理(発生事象管理)</p> <p>データ管理(ストレージ) サービスレベル管理/構成管理/リリース管理/変更管理/キャパシティ管理(資源管理)/ セキュリティ管理/可用性管理(稼働管理)/問題管理/インシデント管理(発生事象管理)/ ITサービス継続性管理</p> <p>ネットワーク管理 サービスレベル管理/構成管理/リリース管理/変更管理/セキュリティ管理/ 可用性管理(稼働管理)/キャパシティ管理(資源管理)/問題管理/ ITサービス継続性管理/インシデント管理(発生事象管理)/</p> <p>ファシリティ管理 サービスレベル管理/構成管理/変更管理/セキュリティ管理 可用性管理(稼働管理)/ITサービス継続性管理/問題管理</p> <p>ITリソース評価項目</p> <p>ファシリティ 建物(構造・基準)/フロア仕様/ラック設備/電源設備/空調設備/ 消火設備/地震対策設備/入退管理設備(セキュリティ)/センタ運用</p> <p>コネクティビティ 通信設備(回線)/通信設備(LAN)/冗長回線サービス(バックアップ)/ セキュリティ/ポート設備</p> <p>コンピュータ 機器仕様/機器構成/システム性能</p> <p>ストレージ 機器構成/システム性能/データ容量</p> <p>アプリケーション システム性能/セキュリティ/ソフトウェア構成/システム保守</p> <p>ミドルウェア システム性能/システム保守/セキュリティ</p>	<ol style="list-style-type: none"> 1.はじめに 2.目的 3.適用範囲 4.葬祭サービスガイドライン遵守事業者の登録及び公表 5.所属員の企業行動原則 6.基本的人権の尊重および顧客情報の守秘義務 7.ご遺族の選択の意思の尊重 8.公正・自由な競争の確保 9.関連法令の遵守 10.情報開示・提供、助言 11.所属員の説明責任 12.相談窓口の設置 13.料金体系の明確化 14.商品・サービス等の商品目録および価格表の提示 15.見積書(施行明細書)交付の義務 16.葬儀施行 17.請求書(施行費用明細書)交付の義務 18.心付け 19.施設・設備の整備 20.安全・衛生の確保 21.トラブル防止および苦情処理態勢の整備調停機関の設置 22.指導・勧告および登録抹消 23.付則

3. 電気通信事業法改正と消費者保護ルール制定の事例

2004年に施行された、改正電気通信事業法は、事業者の多様な事業展開を促すことも目的としている。改正によって第一種、第二種の従来の区分が取り払われ、第一種電気通信事業者に課していた参入、退出における許可取得の要件が緩和された。

図表 改正電気通信事業法の概要

規制項目	現行の規制			新たな規制
	第一種	特別第二種	一般第二種	
事業参入	許可	登録	届出	登録又は届出
事業内容の変更	許可	登録	届出	登録又は届出
事業退出	許可	届出		届出（ただし、利用者への事前周知を義務付け）
料金・契約約款作成、公表義務（サービスに関するルール）	あり	あり	なし	<ul style="list-style-type: none"> ・作成、公表義務を原則廃止（市場支配力を有するサービスについては、「保障契約約款」の作成、公表義務あり）、 ・利用者への重要事項説明義務、苦情処理の義務あり
技術基準	事前の適合確認義務、基準維持義務	事前の適合確認義務、基準維持義務	不要	回線設備を設置する事業者については、基準維持義務あり。基準適合性は、事前に自ら確認する。（自己確認制度の新設）

ガイドライン
の策定

（出所）鈴木賢一「電気通信事業における競争政策」調査と情報 第418号（国立国会図書館、2003年）

退出規制緩和により事業者が事業の休廃止を選択しやすくなったが、突然の休廃止によって消費者が不利益を受けないようにすることや、多様化・複雑化する通信サービスにおける消費者への適切な説明を確保することが必要となった。

総務省は「電気通信事業法の消費者保護ルールに関するガイドライン」を制定し、規制緩和下での消費者保護ルールを提示した。

ガイドラインの要点は以下の通りである。

1) 事業退出に伴う利用者への事前周知

- 1月前までを目途として、利用者には事業の休廃止を周知させること。
- 必要に応じて、代替サービスへの移行に必要な手続等を勘案し、より早い周知が必要。
- 周知の方法は、訪問、電話、郵便等、電子メール、ポータルサイト上での表示のいずれかによる。

- 法令による義務ではないが、望ましい対応として、報道発表、HP、日刊紙への掲載、複数の連絡手段の使用、利用者からの問合せ窓口の紹介、代替サービスの紹介、誠実な対応が挙げられる。

2) 利用者への重要事項説明義務

- 説明対象サービスは「国民の日常生活に係るものとして総務省令で定める電気通信役務」であり、10項目が挙げられている。
- 店舗・街頭で説明を行う際には、ガイドライン規定の説明事項を記した書面を交付。消費者が了解したときに限り、ウェブページ、電子メール、CD-ROM、ダイレクトメール、電話（書面を遅滞なく送付）により説明事項を表示・
- 説明内容は以下の通りである。
 - ① 電気通信事業者の名称
 - ② 電気通信事業者の問合せ連絡先
 - ③ 電機通信サービスの名称及びその種別
 - ④ その利用者に適用される料金
 - ⑤ 契約の変更及び解除
 - ⑥ 特段の制限事項
- 法令による義務ではないが、望ましい対応として、通常の説明では理解が難しい消費者への詳細な説明、詳しい説明を求められた際の対応、未成年者への説明時の配慮、マニュアル作成及び従業員研修の充実が挙げられる。

3) 苦情処理の義務

- 苦情の適切かつ迅速な処理を求めている。
- 「適切かつ迅速な処理」を構成する最低限の条件については以下の通りである。
 - ① 窓口が設置されている。
 - ② 窓口の連絡先や受付時間等が消費者に明らかにされている。
 - ③ 窓口の利用が実際に可能である。

4. 安全・信頼性 WG 等での検討内容の整理

安全・信頼性 WG においては、ASP・SaaS 事業者及び ASP・SaaS サービスの評価に資する情報開示項目として、以下があげられた。

1) ASP・SaaS 事業者の情報開示項目

(※安全・信頼性 WG での指摘事項以外の項目も補足している)

(1) 事業所・事業の概要

①事業所等の概要

- ・事業者名
- ・設立年、事業年数
- ・本店所在地、事業所数、主な事業所の所在地

②事業の概要

- ・事業内容の概要

(2) 人材

①経営者

- ・代表者名、代表者の写真・年齢・経歴（学歴、業務履歴、資格など）
- ・役員数、役員氏名

②従業員

- ・従業員数、うちエンジニア、プログラマー数（有資格者・合格者数とその資格・試験名）

(3) 財務状況

①財務指標

- ・基礎的財務指標（売上高、経常利益、資本金）
- ・安全性財務指標（自己資本比率、キャッシュフロー対有利子負債比率、インタレスト・カバレッジ・レシオ）
- ・貸借対照表、損益計算書、キャッシュフロー計算書

②財務データの確かさ

- ・上場の有無（有の場合は、上場している市場）
- ・財務監査の有無（会計監査人による会計監査／会計参与／中小企業会計によるチェックリスト）
- ・決算公告の有無

(4) 資本関係・取引関係

①資本関係

- ・大株主（上位 5 名）及び株式保有比率

②取引関係

- ・大口取引先
- ・主要取引金融機関
- ・所属団体

(5) コンプライアンス

①組織体制

- ・コンプライアンス担当役員及び学歴・経歴
- ・コンプライアンス専担の部署／会議体
- ・サービスの苦情対応部署、人員数

②文書類、プログラム

- ・情報管理・セキュリティ・運用等に関するポリシー、規程類の整備
- ・勧誘・販売に関する規程等の整備
- ・苦情対応に関する規程等の整備
- ・情報管理・セキュリティ・運用等に関する水準を向上させるためのプログラム

③監査・認証

- ・プライバシーマーク、ISMS、ITSMS の取得状況
- ・18 号監査（米では SAS70）の監査報告書作成の有無

④その他

- ・事業継続計画の有無
- ・インシデント・レスポンス
- ・過去の情報漏洩事故の有無・件数

(6) その他

①CS 活動

- ・可能であれば CS 調査の結果

②CSR 活動

2) ASP・SaaS サービスの情報開示項目

(1) サービス全体

- ①サービスの提供開始年月
- ②サービスの内容・範囲
 - ・明確なサービスの範囲の提示
 - ・サービス事例の公開
 - ・SLA の公開
 - ・約款・契約内容・賠償責任などの明確化
- ③サービス利用量
 - ・利用者ライセンス数（国内・国外）、ライセンスの伸び率公開
 - ・サービス利用中企業数
 - ・取り扱い代理店数
- ④サービスの総合的なレスポンス
 - ・レスポンス向上、またはレスポンス維持のための対策公開
- ⑤サービスの総合的な維持・保守
 - ・連続稼動維持のための対策公開
 - ・保守のための計画停止計画の提示
 - ・計画的な資源増強
 - ・メンテナンス計画・拡張計画
 - ・サービス停止事故の有無（目安としては1時間以上の停止とする）
 - ・予防保守の為の定期的な分析・評価（分析レポートの有無、第三者への依頼等）
 - ・サービスの品質維持（サーバダウン時の復旧時間、予備サーバの有無）
- ⑥サービスの総合的な安全性
 - ・セキュリティ維持に関わる機密情報の保護。利用者個人情報は、改ざん・誤消去・漏洩等が困難な保管システムの導入
- ⑦サービス料金・費用体系
 - ・明確なサービス料金体系の提示
 - ・サービス利用費用の開示有無

(2) アプリケーション

- ①アプリケーションの内容
- ②料金体系
- ③拡張性
 - ・API 等、他システムとの連携方法の提供内容)
- ④セキュリティ

- ・ウイルス対策、DoS などアタック対策
- ・認証
- ・データダウンロード
- ・マルチテナント間セキュリティ

(3) ネットワーク (システム)

① ネットワークの性能・信頼性

- ・提供者側の回線帯域
- ・利用者側に必要な帯域
- ・状況確認 (機器負荷、トラフィックなどをエンドユーザが確認)
- ・接続構成、アクセス経路等のネットワーク、システムの信頼性 (冗長化)

② ネットワークの安全性

- ・外部ネットワークとの接続、内部ネットワーク、システム構成、二重化
外部ネットワークからの不正アクセス、ウイルス攻撃等に対し、それを検知および防御するためのシステム (ファイアウォール等)
- ・利用者と事業者間の安全な通信路の確保 (なりすまし、改ざん、暗号化の対策等)
- ・通信ログ、認証ログ等の非改ざん (完全性) を保証する情報 (電子署名等の手段)
- ・認証方式、暗号方式の採用の有無 (BASIC 方式、ワンタイム方式、デジタル署名方式等)
- ・情報漏えい対策

③ ネットワークの性能監視 (※)

- ・性能監視方法/体制
- ・監視範囲 (ネットワークシステムを構成する全機器が望ましい)
- ・監視項目 (標準的なデータや機器固有のデータなど問題を把握する上で必要なデータ群)
- ・データ収集間隔 (1 分間隔などの詳細インターバルである必要がある)
- ・データ蓄積期間

(※) 性能監視とは、ネットワークシステムを構成するネットワーク機器、サーバ機器などすべてにおいて、均一かつ性能を把握できる詳細なデータを取得し監視・管理することである。

④ システムトラブル処理・再開対策

- ・システムトラブルやシステムの破壊等に対して、緊急停止手段やバックアップデータによる復旧手段を用意すること、業務一時停止・終了時の利用者への事前通知等の手順が明確に定められていること

⑤ 利用インターネットサービスプロバイダの情報

- ・上流 NSP 契約数及び契約帯域数の明示

- ・冗長化対策（論理的、物理的構成）
- ・使用機器の仕様
- ・SLA（パケットロス、パケット遅延、可用性、故障回復時間、過去のSLA違反件数等）
- ・サポート体制、監視体制

（４）サーバ

①性能

- ・ハードウェアスペック、負荷分散

②信頼性

- ・使用ハードウェア（メーカー等）、保守体制

③状況

- ・機器負荷、同時アクセス数などをエンドユーザが確認

④利用方法

- ・シングルテナント or マルチテナント

（５）データセンター（ファシリティ）

①利用データセンター事業者名

②設置場所

③耐震性・耐火性

- ・耐震性・免震性

「地震に対する安全性に係る建築基準法」またはこれに基づく命令、条例の規定に適合するものであること。機器等の固定その他の耐震措置が講じられていること

- ・耐火性

建築基準法に規定する耐火建築物または準耐火建築物であること

④電気設備・消火設備

- ・無停電電源確保
- ・消火設備（緊急火災時に業務の継続を確保できること）

⑤バックアップ体制

- ・データ保管の有無
- ・情報に対するバックアップとその管理は保たれているか
- ・正確な通信記録を作成し、通信状態について通知することが可能であること

⑥セキュリティ

- ・防犯監視対策
- ・破壊侵入防止対策

- ・情報漏えい対策

(6) サービスサポート

①運用サポート

- ・サポート時間の開示 (9:00 から 17:00 or 24h、休日対応等)
- ・サポート手段の開示 (メール、電話、Web、訪問等)
- ・サポート範囲の開示 (ネットワーク調査の可否)

②障害時の保障と対応について (SLA に内包)

- ・サービス停止時の保障の開示 (停止時間と保障額の明示)
- ・サービス停止時の代替手段提供
- ・サービス停止時の緊急連絡

③機器操作・サービス利用サポート

- ・機器操作サポート
- ・API 利用サポート

④利用者への通知、注意事項

- ・サービス一時停止・終了時には事前に利用者へ個別に通知・連絡すること
- ・システムトラブル、システム破壊、災害発生時には障害の発生と復旧見通しについて速やかに利用者に通知すること

⑤事故発生時処理、責任範囲の明確化

- ・事故発生時に、その発生源が特定できること、事業者自身の責任と保証の範囲に関するポリシーを開示すること

5. ASP・SaaS 事業者・サービスの情報開示項目の検討

以上のようなガイドライン参考事例、安全・信頼性 WG での検討、及び「SLA 評価項目と設定値」(ASPIC ジャパン作成)等を総合的に勘案し、ASP・SaaS 事業者・サービスの情報開示項目を検討した。同時に、この情報開示項目は「ASP・SaaS の安全・信頼性に係る情報開示指針(案)」としても活用する予定である。

なお、最終的には、総務省において開催されている「ASP・SaaS の情報セキュリティ対策に関する研究会」の検討結果との整合性を図ることとする。