意見書

平成 20 年 1 月 18 日

総務省情報通信政策局
　情報セキュリティ対策室　殿

郵便番号　105-7316
（ふりがな）とうきょうとみなとくひがししんばし
住　　所　東京都港区東新橋一丁目 9 番 1 号
（ふりがな）かぶしきがいしゃ
氏　　名　ソフトバンクテレコム株式会社
だいひょうとりしまりやくしゃちょうしーいーおー　そん　まさよし
代表取締役社長ＣＥＯ　孫　正義

「ASP・SaaS における情報セキュリティ対策ガイドライン（案）」に関し、別紙のとおり意見を提出します。

別紙

このたびは、ASP・SaaS における情報セキュリティ対策ガイドライン（案）等に係る意見募集に関し、意見提出の機会を設けて頂いたことにつきまして、御礼申し上げます。

以下のとおり弊社共の意見を述べさせて頂きますので、宜しくお取り計らいの程、お願い申し上げます。

「評価項目」の削除

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と考えます。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ります。また、サービス提供価格の高騰に繋がることが危惧されます。以下に一例を挙げます。III.1.1.6（P.40）において、脆弱性パッチ更新作業着手までの時間（対策参照値）が提示されていますが、パッチ適用に際しては、そのパッチ自体の動作検証にも時間を要するため、検証に要する時間を一律に定められるものではないと考えます。

PDCA の概念において、こうした評価項目・対策参照値の設定は、あくまでもその起点としての基準となるのみと考えます。また、技術動向・脅威の変化に伴い見直しは必須となります。総務省の名義でこうした静的な規準を与えてしまうことが「これだけやっていれば大丈夫」といった ASP・SaaS 業界の安易なリスク認識・セキュリティ対策に繋がることを懸念します。

評価項目・対策参照値のような基準を定めるならば、評価項目・対策参照値のタイムリーかつ継続的な見直しが必要不可欠です。こうした役割は民間の中立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です。

事業者間でセキュリティレベルを評価しあう必要性

当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はありません。複数のアプリケーションサービスが連携して一つのサービスをユーザに提供するケース（所謂「マッシュアップ」）においては、ユーザに提供されるセキュリティレベルは関与するサービスのうちでもっとも低いセキュリティレベルのものに引きずられます。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と考えます。

ガイドラインの構成に関して

　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です。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と考えます。

以上