ASP・SaaS の情報セキュリティ対策に関する研究会
（第 3 回会合） 議事要旨（案）

1．日　時：平成 19 年 10 月 17 日（水）15:00～17:00

2．場　所：三田共用会議所　3 階 C・D・E 会議室

3．出席者

(1) 構成員 （座席順、敬称略）

座長：佐々木良一（東京電機大学）

座長代理：中尾康二（KDDI株式会社）、藤本正代（情報セキュリティ大学院大学）

構成員：青木英司（日本電気株式会社）、今田正実（株式会社富士通ビジネスシステム）、上原稲一（沖縄電力株式会社）、及川喜之（株式会社セールスフォースドットコム）、小倉博行（三菱電機株式会社）、木村隆司（ブレイン株式会社）、小林慎太郎（株式会社野村総合研究所）、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・ジャパン）、西山敏雄（NTTコミュニケーションズ株式会社）、花戸俊介（トライコーン株式会社）、宮坂肇（株式会社 NTT データ）

欠席構成員：松橋義樹（株式会社サンスイ）、林敏（ミロク情報サービス）、岩下安男（株式会社大阪エクセレント・アイ・ディ・シー）

(2) 総務省

河内情報セキュリティ対策室長、村上情報セキュリティ対策室課長補佐、中村情報セキュリティ対策室課長補佐、山下電気通信技術システム課課長補佐、田邉情報セキュリティ対策室対策係長、中尾情報セキュリティ対策室国際政策係長

4．議事概要

(1) 開会

(2) 配付資料の確認

(3) 前回会合の議事要旨の確認

資料 3-1 に基づき、前回会合の議事要旨が確認された。

(4) 構成員の出欠確認

(5) 議事

① ASP・SaaS における情報セキュリティ対策の現状・課題について

資料 3-2 に基づき小倉構成員より ASP・SaaS における情報セキュリティ対策の現状・課題について三菱電機株式会社における事例をもとに説明が行われた。

② ASP・SaaS における情報セキュリティ対策の現状・課題について

資料 3-3 に基づき木村構成員より ASP・SaaS における情報セキュリティ対策の現状・課題についてブレイン株式会社における事例をもとに説明が行われた。

③ ASP・SaaS の情報セキュリティ対策ガイドライン（たたき台）の検討

資料 3-4、資料 3-5、資料 3-6-1、資料 3-6-2 に基づき事務局より ASP・SaaS における情

報セキュリティ対策ガイドライン等に関する説明が行われた。要旨は以下のとおり。

- ASP・SaaS のサービス種別を分類し、機密性・完全性・可用性の観点から 12 のパターンに振り分けた。機密性の観点であれば個人情報の扱い、完全性については財務上・会計上の扱いを中心に考え、可用性の観点からは復旧時間を重視して分類した。
- ガイドラインの組織・運用編では、PDCA、業務・事業者間の連携、SLA 等の特性を考慮し、分類した 12 パターンに共通のガイドラインとしてはどうかと考えている。
- ガイドラインの物理的・技術的対策編では、機密性・完全性・可用性の観点でリスク分析を行い、各セキュリティ対策がどのリスクに対応するかの分析を行った。
- また、原則実施すべき「基本」対策であるのか、追加的に実施する「推奨」対策であるのかについても分析した。
- 今後、12 パターンの対策について、機密性・完全性・可用性の重要度に応じた適切なレベル感を出すため、各対策の評価項目に対する基準値、すなわち要求されるレベルがどの程度かを検討する必要がある。

事務局から、ASP・SaaS の情報セキュリティ対策ガイドラインの詳細検討を行うボランティアベースの WG 設置が提案され、構成員により承認された。

④ 自由討議

事務局より以下の論点が示され、当該論点に沿って討議が行われた。

論点 1: セキュリティ対策を3つの判定要素(機密性・完全性・可用性)により分類したが、適当か。(他の判定要素は必要ないか。)

論点 2: 12 パターンという分類数は妥当か。(統合して減らすべきか。)

論点 3: 各対策項目を、「基本」と「推奨」に分けるのは適当か。

論点 4: 対策項目は同じでも、求められる遵守レベルが異なる場合に、「評価項目」とその「基準値」を用いてレベル感を表すのは適当か。

論点 5: ガイドライン全体の構成を「組織・運用編」と「物理的・技術的対策編」の 2 部構成とするのは適当か。

論点 6: その他(実際に利用する上でのボリューム感、内容・構成の分かりやすさ等)

主な意見・質疑は以下のとおり。

＜ガイドラインの目的・趣旨に関する意見＞

- ガイドライン策定の狙いは、情報セキュリティに対する知識が乏しい ASP・SaaS 事業者に対し、自社の事業内容に応じて必要なセキュリティ対策を選択することができるよう、情報セキュリティ対策をパターン化すること。
- ASP・SaaS 事業者だけでなく、いかにユーザーに普及させるかということも課題。
- 中小の ASP・SaaS 事業者にとっては、言葉及び内容が複雑すぎると思われる。もう少し理解しやすいものに改善すべき。
- 「組織・運用編」と「物理的・技術的対策編」の 2 つに分けてガイドライン化することには賛成である。

＜組織・運用編に関する意見【論点 5 関連】＞

- ISO/IEC27001 の内容は要求事項であり、ガイドラインではない。内容を変更すべきではない。
- ISMS の大きな課題は、133 のコントロールにインプリメントガイドラインが多く記載されているため、コンサルタント委託等の大きなコストが必要と思われることである。
- ASP・SaaS 事業において、ISMS に書かれている対策をすべて実施する必要がある訳ではない。ガイドラインの在り方の一例として、ISMS を ASP・SaaS 事業者が適用する際の簡素化の考え方や対策を定めるという方法もある。

＜物理的・技術的対策編に関する意見【論点 1～4 関連】＞

- 対策パターン数は、より少なくする方が望ましい。
- 資料 3-6-2（P.3）第 3 章は、ASP・SaaS 事業者にとって対策を講じようのないインターネットデータセンター（IDC）に関する事項である。このように、事実上ほとんどの場合がアウトソースに依存する部分については、その旨の解説を加えるべき。

(6) その他

事務局より次回会合についての予定が説明された。

(7) 閉会

以 上