ASP・SaaS の情報セキュリティ対策に関する研究会
（第 4 回会合） 議事要旨（案）

1．日時：平成 19 年 12 月 18 日（火）10:00～11:00

2．場所：三田共用会議所　第 3 特別会議室

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）、岩下安男（株式会社大阪エクセレント・アイ・ディ・シー）、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）、松橋義樹（株式会社サンスイ）、宮坂肇（株式会社 NTT データ）

欠席構成員： 林敏（ミロク情報サービス）、上原稲一（沖縄電力株式会社）

(2) 総務省

中田政策統括官、松井官房審議官、鈴木総合政策課長、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、中里情報通信政策課課長補佐、吉田データ通信課課長補佐、渡辺電気通信技術システム課主査、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) 冒頭挨拶　中田統括官

中田統括官より挨拶が述べられた。

(3) 配付資料の確認

(4) 前回会合の議事要旨の確認

資料 4-1 に基づき、前回会合の議事要旨が確認された。

(5) 構成員の欠席確認

(6) 議事

① 事務局より、資料 4-2「ASP・SaaS における情報セキュリティ対策ガイドライン（案）」に基づき説明が行われた。質疑応答を踏まえて修正することで、パブリックコメントにかけることが承認された。

② 事務局より、資料 4-4「ASP・SaaS の情報セキュリティ対策に関する研究会報告書（案）」について、資料 4-3「同報告書要旨（案）」に基づいて説明が行われた。質疑応答を踏まえて修正することで報告書（案）をパブリックコメントにかけることが承認された。

- **資料 4-2「ASP・SaaS における情報セキュリティ対策ガイドライン（案）」に基づく説明の要旨は以下のとおり。**

・ 本ガイドラインは、ASP・SaaS 事業者が実施すべき情報セキュリティ対策を取りまとめたものであり、「Ⅰ 序編」、「Ⅱ 組織・運用編」、「Ⅲ 物理的・技術的対策編」の 3 編構成。
・ 本ガイドラインの活用により、次のような効果が見込まれる。
  ① 人的・金銭的な資源を割く事が困難な中小企業の ASP・SaaS 事業者に対し、独自の脅威分析の負担を軽減し、優先的に取り組むべき対策の指針を与えること
  ② 他の ASP・SaaS 事業者と連携する場合、その事業者に対する情報セキュリティ対策の要求事項として、本ガイドラインが一定の指針となること
  ③ 利用者が ASP・SaaS サービスを選択する際の指標となること
・ 「Ⅰ 序編」は、本ガイドラインの目的、対象範囲、利用方法、注意事項、用語の定義等をまとめた導入編。
・ 「Ⅱ 組織・運用編」は、経営者等の組織管理者のために、運用管理体制のあり方、外部組織との契約における留意事項、利用者に対する責任等をまとめた対策集。
・ 「Ⅲ 物理的・技術的対策編」は、ASP・SaaS の情報資産に対する情報セキュリティ対策集であり、主に ASP・SaaS サービスを運用する現場の技術者向け。
・ ASP・SaaS サービスを機密性・完全性・可用性の観点からサービスを 6 パターンに分類し、各パターンに適合する情報セキュリティ対策レベルを提示。
・ 情報セキュリティ対策を「基本」と「推奨」に分類し、実施の優先度を提示するとともに、実施においての参考事例であるベストプラクティスを加えた。
・ 物理的・技術的対策には、対策項目の実施レベルを定量的・具体的に評価するための評価項目を設けた。また、各評価項目に、対策項目の実施レベルの目安となる対策参照値をパターン毎に設定した。対策参照値に*（アスタリスク）が付されているものは、情報セキュリティ対策上、特に達成する必要がある値である。

本説明についての質疑応答は以下の通り。

- 53 ページの「アクセス認証方法」など、対策参照値の欄に 2 つの値が並べて書いてあるものがある。この場合、「and」なのか「or」なのかを明示すべき。

（事務局回答） 複数の対策参照値が意味するところを十分に精査した上で、「and」条件なのか「or」条件なのかを明示したい。

- 用語の定義において、JIS Q 13335-1 を参照しているものがあるが、現在、当該規格は統合・改編中であるため、規格番号が変更又は消滅する可能性がある。混乱を避けるため、

JIS Q 27001 のみの引用で十分ではないか。

（事務局回答） ご指摘のとおり修正したい。

- 「Ⅰ　序編」の中にガイドラインの全体構成について記述されているが、序編自体についても触れられており違和感がある。全体構成は序編の前に記述するべきではないか。

（事務局回答） 読者の読みやすさ・理解しやすさに配慮して、構成の複雑化をできるだけ避けるため原案のままとしたいので、ご理解願いたい。

- **資料 4-3「ASP・SaaS の情報セキュリティ対策に関する研究会報告書要旨（案）」に基づく説明の要旨は以下のとおり。**

・ ASP・SaaS サービスは、提供する事業者に顧客企業の膨大な機密情報や個人情報が集積する特性があるため、健全に発展していくためには情報セキュリティ対策が不可欠。
・ その他にも、人的・金銭的資源に限りがある場合の情報セキュリティ対策の優先度付けができていない、多岐に渡るサービスの特徴に基づく適切な情報セキュリティ対策が実施できていない、利用者に対し十分な説明や情報開示が行われていない等の問題意識がある。
・ 既存の基準やガイドラインは、ASP・SaaS サービスの特性を念頭に置いて作成されていないため、ASP・SaaS サービスに適合した情報セキュリティ対策ガイドラインが必要。
・ 本ガイドラインの策定に際し、以下の 4 点に重点化。
　① ASP・SaaS 事業者が優先的に取り組むべき情報セキュリティ対策を絞り込むこと
　② 簡単にサービスに即した情報セキュリティ対策実施が可能となること
　③ 理解及び実施しやすい具体的な情報セキュリティ対策を示すこと
　④ 利用者にとっても理解しやすいものであること
・ 本ガイドライン策定に際し、7 点の具体的アプローチを検討。
　① ASP・SaaS の典型的なシステム構成に基づき、ASP・SaaS サービスの特性に特化した情報セキュリティ対策を導出
　② 実施すべき基本的な対策と、実施が推奨される対策に分類
　③ 分かりやすい記述、定量的あるいは具体的な対策実施レベルの目安を提示（特に達成が必要とされる対策レベルは区別し明示）
　④ ASP・SaaS 事業者の課題と判明した組織運用に関するセキュリティ対策も用意
　⑤ サービス毎のセキュリティ要件に基づいたパターン分類を用い、網羅性と適合性を確保
　⑥ パターンを用い、サービスに適した対策を容易に選択できるアプローチを設定
・ 今後の課題は、まず、本ガイドラインが広く認知・活用されること。また、技術の進歩等により内容が ASP・SaaS サービスの実態にそぐわなくなることを防ぐため、ガイドラインを定期的、継続的に見直し・改善する体制を構築すること。

本説明についての質疑応答は以下の通り。

- パブリックコメントの対象はどの資料か。

（事務局回答） 資料 4-2 のガイドライン（案）及び資料 4-4 の報告書（案）。資料 4-3 の報告書要旨（案）は、参考資料として報道資料等に添付する予定。

- ガイドラインの利活用効果として、「適切な情報セキュリティ対策が施された ASP・SaaS サービスの導入により、利用者の総合的な情報セキュリティ環境の改善が可能になる」という一文を追加してほしい。

（事務局回答） ご指摘の主旨は、既に報告書（案）の序章・第１章に記述しているところであるが、第4章のガイドラインの利活用効果の項への追記を検討したい。

- 資料4－3の6ページ、「既存の法令・基準・ガイドライン等」における凡例の色分けが間違っているので修正願いたい。

（事務局回答） 確認の上、必要な修正を行いたい。

- 検討過程で、JIS Q 20000 シリーズの一部（IT サービスに関する部分）を参考にするという考え方があったと思うが、現在のガイドライン（案）に反映されているのか。

（事務局回答） 専門家を交えて詳細な検討を行なったところ、ISO/IEC 27001 及び 27002 の外部組織に対する契約の部分の記述で代替・網羅できるという結論となったため、結果として JIS Q 20000 シリーズを参考とはしていない。

(7) その他

事務局より、パブリックコメントを 12 月 19 日から来年 1 月 18 日まで実施する予定であることが説明された。また、第5回会合は、パブリックコメントにおける意見の提出状況を踏まえ、1 月下旬または 2 月上旬を目処に調整していく予定であることが周知された。

(8) 閉会

以上