ASP・SaaS の情報セキュリティ対策に関する研究会
（第 2 回会合） 議事要旨

１．日時：平成 19 年 8 月 8 日（水）10:00～12:00

２．場所：三田共用会議所　3 階 A・B 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）、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）、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（株式会社ミロク情報サービス）

(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、吉田データ通信課課長補佐、山下電気通信技術システム課課長補佐（代理　山中安全・信頼性対策係長）、田邉情報セキュリティ対策室対策係長

４．議事概要

(1) 開会

(2) 配付資料の確認

(3) 議事

① 前回会合の議事録要旨の確認

② 構成員の紹介（事務局の交代）

③ 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 2-2 に基づき、宮坂構成員（説明は、守屋氏）より ASP サービス事例紹介として NTT データの CO_2ナビゲーターについての説明が行われた。

本件に関する質疑応答の要旨は、以下のとおり。

・ NTT データでは、全社のセキュリティポリシーを策定済みで、かつ ASP サービスに関しても全社のセキュリティポリシーに基づく形で実施手順を策定している。

・ 社内で運用のばらつきが出るのを防ぐため、国際的に認知度の高い ITIL と CMMI を活用し、全社の基準として運用管理実施要領を策定している。

④　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 2-3 に基づき、花戸構成員よりトライコーン社における ASP・SaaS における情報セキュリティ対策の現状と課題について説明が行われた。

本件に関する質疑応答の要旨は以下のとおり。

・ セキュリティレベルの向上にあたっては、コストバランスを踏まえつつ、物理的な安全性、プログラムの安全性、運営する人間・会社の安全性の 3 つをバランスよく高めていくことが重要。

・ ユーザは法人限定であり、情報セキュリティに関しては機密性を最も求められることから、ISO・P マークの取得や脆弱性診断に注力している。

⑤　事務局説明

以下の資料に基づき、事務局より説明を行った。

- 情報セキュリティ対策に関連する基準・ガイドラインの現状・課題について（資料 2-4）
- ASP・SaaS の情報セキュリティガイドライン検討に向けての論点整理（資料 2-5）
- ASP・SaaS の情報セキュリティガイドラインの検討方法について（資料 2-6）

⑥　自由討議

上記事務局説明に基づいて意見交換が行われた。要旨を以下に示す。

・ 資料 2-5 の p.3、13 及び 16 に以下のキーワードを追加してほしい。
- ASP・SaaS ベンダーとユーザ間のリスクコミュニケーションが必要。
- ASP・SaaS ベンダーとユーザが共に理解できる言葉で書かれたガイドラインを策定する視点が必要で、共有することが大切。

・ 新ガイドラインで重要なのは、以下の 3 点。
- ガイドラインの遵守が、認定マーク取得により担保されていること。
- ユーザから見て、ガイドラインの適用範囲が容易に識別できること。
- 審査基準として利用すること。

・ 新ガイドラインは、役所の審査基準として利用するのではなく、ASP・SaaS ベンダーを中心とする業界団体の取組みのなかで活用されることを主眼にしている。また、情報セキュリティ対策の必要最低限のガイドラインとして考えたい。

・ 電気通信分野における情報セキュリティ対策協議会（総務省はオブザーバとして参加）において ISM-TG（電気通信事業における情報セキュリティマネジメントガイドライン）について議論されており、ISM-TG を取得した電気通信事業者に対し、ISMS に加え、T マークという新認証マークを表示する方向で調整している。同様に、本研究会で策定する新ガイドラインについても、ASP・SaaS 特有の要件を満たすものとして、既存の ISMS に追加する形で新たな認証マークを付与することもできるのではないか。

・ ISP-ISP 間の情報セキュリティ対策については、ISO/IEC27001 に記載されていないため、新ガイドラインに対する要求事項を明確にしておく必要がある。

・ 政府の経済財政諮問会議の論点には、中小企業の生産性向上のために ASP・SaaS を促進するという議論はあったが、中小 ASP 事業者の振興の観点は無かったと認識。認証制度を検討する際は、ASP 事業は装置産業であり、中小事業者は次第に淘汰・集約されるという視点も必要ではないか。
・ 必要最小限のセキュリティ対策ではなく、業界で守るべき一定のセキュリティレベルとして合意できるラインを検討すべきである。
・ 最低ラインのセキュリティ対策（must の部分）を明確にし、かつ ASP・SaaS ベンダーとユーザが SLA で用いているような数値を共通化したガイドライン（want の部分）を推進していく必要があると考える。
・ 資料 2-6 p.2 にある MICTS については、MICTS-1 の一部が、ISO/IEC 27000（Fundamentals and vocabulary）になり、MICTS-2 が ISO/IEC 27005(Information security risk management)のファイナルドラフトとなっており、本研究会限りということであれば参考資料として提供可能である。また、ITU に提案している我が国の ISM-TG を反映した勧告 X.1051 改訂版も同様に提供可能である。

(4) その他

事務局より次回議会の会合についての予定が説明された。

(5) 閉会

以上