ASP･SaaSに対する情報セキュリティ監査をふまえたクラウドコンピューティングに対する一考察

A study on Cloud computing
based on information security audit for ASP･SaaS

情報システム監査株式会社
佐々木 志津香･ 古江 健一･鬼松 嵩

はじめに

近年、クラウドコンピューティングが急速に普及しつつある

メリットの反面，特有のリスクが存在する

当社の監査実績・調査をもとに

本格的なクラウド時代に向けての情報セキュリティ監査について考察した

目次

1．クラウドコンピューティング
　　特徴・利便性とセキュリティ面の不安

2．ASP・SaaSに対する情報セキュリティ監査
　　（監査実績を基にしたモデルケース）

3．クラウドコンピューティングにおける
　　情報セキュリティ監査の課題

クラウドコンピューティング

- ネットワーク経由でハードウェア・ソフトウェアをサービスとして利用する仕組み

- サービス形態による分類

SaaS ：Software as a Service	アプリケーションを利用 ≒ASP（Application Service Provider）
PaaS ：Platform as a Service	開発環境を含むアプリケーションとプラットフォームを利用
IaaS ：Infrastructure as a Service	仮想化されたサーバー、ストレージ、ネットワークを利用

クラウドのメリットと特殊性

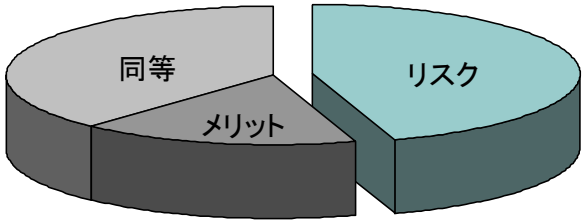
- クラウドのメリット
  - コストの安さ（初期費用・運用管理費用）
  - 開発期間の短縮　etc

- クラウドの特殊性
  - 自前でシステムを持たない（アウトソーシング）
  - ネットワークを通じてシステムを利用する
  - 多数の利用者が基盤を共有する

  ⇒特有のセキュリティリスク

セキュリティ面の不安

- 「クラウドのメリットとリスクどちらが大きいか？」
  - 「リスクのほうが大きい」 45%
  - 「同等」 38%
  - 「メリットのほうが大きい」 17%



ISACA（2010.3）

- 「クラウドを利用する際の懸念事項」
  - セキュリティ対策への不安が最多

経済産業省（2009.5）

- セキュリティ面での不安を持つ利用者が多い

２．ASP・SaaSに対する情報セキュリティ監査
～監査実績を基にしたモデルケース～

１．既存システムからASPサービスへの移行

２．ASP提供業者とのSLA契約の評価

３．ASP事業者で問題が発生しているケース

４．インフラを借用したケース

モデルケース1
既存システムからASPへの移行

- ASP事業者のシステム運用を点検評価

- 重要情報の委託
  - 事業者に問題がないかを第三者が
    点検・評価することが望ましい

セキュリティ監査実施の流れ（1／2）

1．現状システムの把握/分析

- システム運用組織体制・構成図・障害連絡網…
- 問題意識と突き合わせ、監査のポイントを整理

2．現地監査項目の作成

- 公的な監査ガイドラインから、関連項目を選定
- 両者のセキュリティポリシー、実施手順書
- 現状システムの分析で把握した観点

セキュリティ監査実施の流れ（2／2）

3．現地調査

- ドキュメント調査
- 運用管理担当者へのインタビュー
- データセンターの現地視察
- 技術診断（アタックテスト）

4．評価・分析・監査報告

- 調査結果から問題点を分析、原因と対策を検討
- 検討結果を監査報告書に集約
- 監査報告会を実施（利用者側，提供業者側出席）

モデルケース2
ASP提供業者とのSLA契約の評価

SLA契約

- アウトソーシングにおいて重要な要素
  ⇒ASP・SaaSサービスにおいても重要

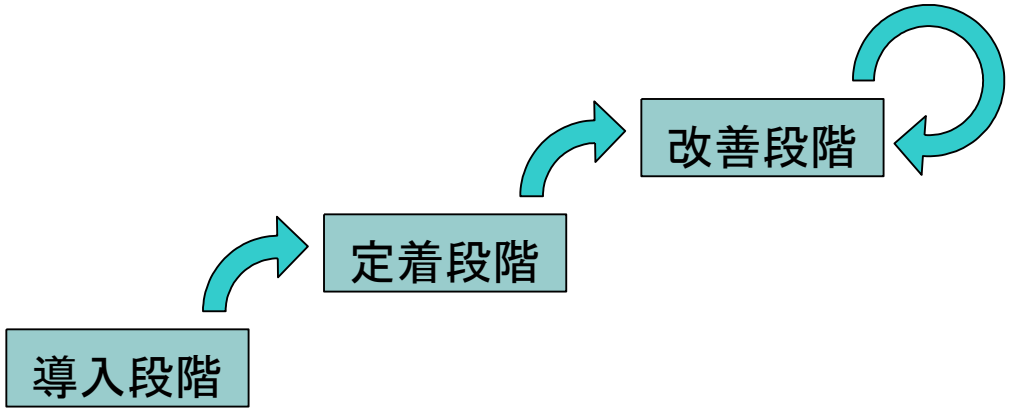
  - SLA (Service Level Agreement)
    - サービス提供者/利用者間でのサービス水準に関する合意
    - サービスの内容・範囲・品質・達成目標などを記述
    - SLAを有効に機能させる仕組みを構築・運営

      ⇒SLM (Service Level Management)

サービスレベルの評価

- SLAに基づいたSLMの構築・運営により
  - サービス利用者
    - 期待通りのサービスを享受
  - サービス提供者
    - 提供責任の明確化、適切な対応の証明

- 継続的な管理を行いサービスレベルを改善



評価実施の流れ（1／2）
～SLAの評価と分析～

1. 予備調査と分析
   - 契約書の入手と分析
   - サービスレベル関連の報告書、測定方法の分析

2. SLA評価項目の妥当性の検証
   - 公的ガイドラインからSLA契約書の評価項目を洗い出し、契約書の項目評価判定を実施

3. SLA契約書の改善案検討

4. 報告書の作成と報告会

評価実施の流れ(2／2)
～評価後の改善提言～

1．SLA契約の見直し提言

- 誤解を与える用語の見直し
- レスポンス計測方法・数値化に関する見直し

2．　SLA定着化への提言

- マネジメントサイクルを確立するための方策提言
  - 体制改善(SLM 委員会の設置等)

モデルケース3
ASP業者で問題が発生しているケース

- ASP事業者で実際に問題が発生している事例を想定

セキュリティ監査実施の流れ（1／2）

1. 問題点の把握
   - インフラ・アプリケーション構成・障害管理表・システム変更履歴から問題発生原因を推測
2. 現地監査項目の作成
   - 把握した概要と公的ガイドラインからの項目
     - サービスの契約内容
     - 安定稼動
     - 機密保護
     - アクセス権管理
   - 推測した問題発生原因をふまえた調査項目

セキュリティ監査実施の流れ（2／2）

3．現地調査

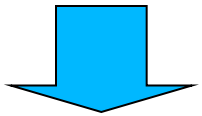
- ドキュメント調査
- 運用管理担当者へのインタビュー
- データセンターの現地視察
- 技術診断（アタックテスト）

4．評価・分析・監査報告

- 調査結果から問題点を分析、原因と対策を検討
- 検討結果を監査報告書に集約
- 監査報告会を実施（利用者側、提供業者側出席）

モデルケース4
インフラを借用したケース

- インフラを自社持ちとせず、ASP事業者へシステム運用まで委託を想定



通常のセキュリティ監査を行う。
但しASP事業者の監査への協力は必須である。

ASP・SaaSに対する情報セキュリティ監査 ～まとめ～

- 通常のセキュリティ監査と同様に実施
  - 既存のガイドラインを柔軟に組み合わせる
- 監査のための契約は必須
  - 監査協力に関しての契約が存在しない場合
    監査実施困難

3. クラウドコンピューティングにおける情報セキュリティ監査の課題

クラウドの様々なセキュリティ課題

	アーキテクチャ	統制・マネジメント	運用・オペレーション	利活用
情報セキュリティ	・分散コンピューティング障害 ・分散メモリ/ストレージ障害 ・バックボーンNW障害 ・仮想化環境のセキュリティ	・統合リスク管理/セキュリティガバナンス ・情報のライフサイクル管理 ・物理的アクセス管理	・パッチ/バージョン/インベントリ管理(脆弱性対策) ・アプリケーションセキュリティ ・インシデントレスポンス ・暗号化と鍵管理 ・ポータルのハッキング対策	・端末のセキュリティ ・通信路のセキュリティ(可用性) ・マッシュアップのセキュリティ ・データポータビリティ ・相互運用性
コンプライアンス	・地政学リスク対策(設置場所) ・データ/プロセスの隔離	・システム/業務監査 ・地政学リスク対策 ・電子フォレンジック	・オペレータのアクセス管理 ・データ/プロセスの隔離	・利用契約SLA ・利用者のアクセス管理 ・地政学的リスク対策(保管・運用場所指定)
個人情報保護	・地政学リスク対策 ・データ/プロセスの隔離	・情報のライフサイクル管理 ・アクセス権限管理	・オペレータのアクセス管理	・利用者のアクセス管理 ・通信路のセキュリティ ・端末のセキュリティ
事業継続管理	・二重化/冗長化	・事業継続計画	・システム障害対策/二重化 ・MTBF、MTTR ・災害復旧計画	・データのローカルバックアップ ・データロックインリスク

情報セキュリティ監査に関連が深い内容

＋

監査実績・調査結果

クラウドコンピューティングにおける情報セキュリティ監査の課題（1／3）

- 事業者の監査協力
  - 監査への対応条件を明確にしておく

- データの保管場所
  - 海外にデータがある場合、現地の法律が適用
    - 米国：パトリオット法　　⇒　データの強制開示？
    - EU　：プライバシー保護　　⇒　個人情報持ち出し制限

クラウドコンピューティングにおける情報セキュリティ監査の課題（2／3）

- データのインテグリティ維持
  - クラウド特有の技術（ex. Key-Value　ストア型DB）
    - 一貫性の保証が弱い⇒基準に適合しない？

- 委託先の監督責任
  - データの安全性は利用者が責任を持つ
    - ex. 個人情報保護法 第22条「委託先の監督義務」

クラウドコンピューティングにおける情報セキュリティ監査の課題（3／3）

- 利用者間の環境の分離（仮想化技術の利用）
  - 複数の利用者が環境を共有するリスク
    - 情報漏洩
    - 不正アクセス
    - 許容能力オーバーによるシステムダウン
- 効率的な監査の実施
  - 利用者ごとに監査を行うのは非効率
  - 共通的な監査の仕組み（ ex.SAS70 ，18号監査）
  - 評価基準（公的認証）

必要と考えられる監査項目の例

- 監査実施、資料の提供に関しての取り決めが契約書に明記されているか
- データの保管場所が明確になっているか
- データの一貫性が、要求水準を満たすか
- 利用者間の環境が適切に分離されているか
- 公的認証を取得しているか

まとめ

- ASP・SaaSの監査も基本的には通常の
  セキュリティ監査と同様
  - 業務委託（アウトソース）の基準などと組み合わせ
  - システムの特性に応じての使い分け
- 本格的なクラウドの監査のために

  今後クラウドサービスは、種々な形態が提供され
  利用されていくと考えられ、それに応じて適格で
  柔軟な、また高度な監査が要求される。なおこの
  4月に経済産業省からクラウド利用面からのガイド
  ラインが公表された、有効な活用を考えて行きたい。

ご清聴ありがとうございました

情報システム監査株式会社
鬼松 嵩・古江 健一・佐々木 志津香