クラウド環境でのセキュリティの捉え方

－セキュリティの視点によるクラウド導入の道標－

アブストラクト

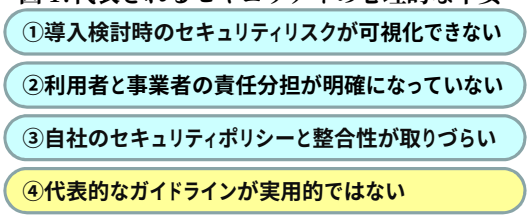
1．研究の背景

近年、クラウドコンピューティング(以下、クラウド)サービスは国内外で注目を集めており、クラウドサービスを利用している企業、利用を検討している企業は年々増加している。しかし、そういったクラウドサービスへの期待がありながら、導入まで至っていない企業が依然として多いのが実状である。本分科会でも導入は 16 社中 3 社に留まっており、クラウドサービスへの期待に比べ、阻害要因の存在が大きいことが窺える。

2．阻害要因の分析

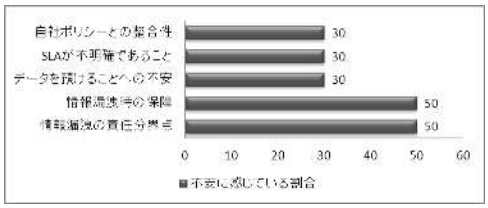
企業のクラウドサービス導入に際して阻害要因を調査したところ、数多くの心理的な不安が挙がった。中でもセキュリティについては、特に 4 件に代表される心理的な不安（図 1）がクラウドサービス導入の阻害要因になっているという現状も明らかになってきた。

図 1.代表されるセキュリティの心理的な不安



また、本分科会で 19 社、119 名に対し、クラウドサービス導入における心理的な不安を調査するためアンケートを実施し、上記 4 件の阻害要因は重要であることが確認できた。

図 2.アンケート結果



3．課題定義／仮説立案

阻害要因を払拭するための検討の過程で、オンプレミス（ユーザーが管理する施設内で導入・運用）とクラウドサービスとではセキュリティの検討をするフェーズの違いが、心理的不安を発生させる一つの要因であると考えた。

オンプレミスで要件定義・設計フェーズで実施していたセキュリティの検討は、クラウドサービスでは導入検討の段階で実施しなければいけない。さらに、クラウドサービス導入では、ユーザーが今までオンプレミスで培ってきたシステム導入のノウハウがそのまま使えない。このため、クラウド導入検討の負荷が高くなっている。

そこで、本分科会は以下の仮説を立案した。

「セキュリティの心理的な不安を払拭するためには導入プロセスを確立する必要がある」

この仮説を立証すべく研究を進めた。

4．クラウドサービス適合性評価プロセスの立案

クラウドサービス導入にあたっては、導入前に機能要件、非機能要件、およびそれに紐付くリスク項目を踏まえて検討する必要がある。短期間に抜けがないよう導入検討を進めるためには全体を俯瞰して見られるプロセスの策定が必要である。そこで、メンバー各社のシステム導入プロセスを比較・分析し、「クラウドサービス適合性評価プロセス」（図 3）を立案した。

以下、このプロセスをシステム検討フェーズとシステム評価フェーズに分けて説明する。

図 3.クラウドサービス
適合性評価プロセス

5．システム検討フェーズの研究

システム検討フェーズではセキュリティリスク優先順位付けのため、セキュリティリスクに紐付くシステム特性・要件を明確にする。当フェーズは次の 2 つのステップで構成される。

Step1：対象業務システムの選定

どの業務システムをクラウドに移行できるかを選定する。

Step2：業務システムの特性分析

対象業務システムの特性により優先順位を付けセキュリティ要件を絞り込む。

Step2 において、クラウドサービス導入を検討する際に、すべての業務システムで多数あるセキュリティ要件すべてを評価していては、検討に時間がかかりすぎることが問題となった。そこで本分科会では、参加企業の 16 社 37 システムを対象に、ISO/IEC9126（ソフトウェアの品質特性モデル）を参考としクラウド導入に重要視されるシステム要件を抽出した。その結果、クラウドのセキュリティを検討する上で重要となる要件を、最終的に 7 項目（「移植性」「拡張性」「可用性」「完全性」「機密性」「信頼性」「コンプライアンス」）に集約し、対象業務システムの特性分析にかかる負荷を軽減させた。

6．システム評価フェーズの研究

システム評価フェーズではガイドラインから読み取りづらいセキュリティリスクの優先順位と責任分担を明確にする。当フェーズは次の 3 つのステップで構成される。

Step3：リスク項目・優先度の明確化

特性分析結果をもとに、リスク項目の優先度を明確にする。

Step4：リスク対応者の責任分担明確化

リスク項目に対し、利用者か事業者のどちらが対応すべきかを明確にする。

Step5：リスク対応状況の評価

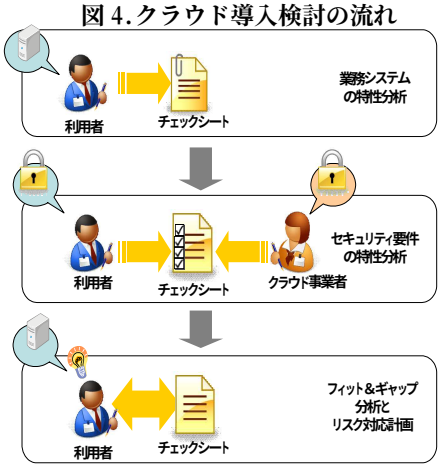
利用者と事業者で対応状況を明らかにし、対応が出来ていないリスクを評価する。

このフェーズでは、既存のガイドラインをそのままではセキュリティリスクを評価しづらい点が問題となった。何のガイドラインをベースにして、どのように非機能要件を結びつけ、評価するかを決める必要があった。そこで、数あるガイドラインの中から何を選択するかを検討し、リスクと脆弱性の対応関係が明確という点で ENISA のガイドラインを選定した。次に、選定した ENISA のガイドラインが利用者に高いセキュリティ知識を要求する点について、本分科会メンバーで内容を読み取りやすくした。さらに、非機能要件と該当する脆弱性を紐付けるため、本分科会メンバーでその紐付けを実施した。最後に、経済産業省のガイドラインを分析しリスク項目とそれに対応する責任分担を明確にした。

7.導入プロセス負荷軽減のためのツール開発と評価

本分科会ではクラウドサービス適合性評価プロセスを導き出すことで、クラウドサービスのセキュリティリスクを可視化することに成功した。しかし、その作業負荷は想定していたよりもかなり多いことが分かった。そこで、非機能要件とセキュリティ要件に関する質問事項に回答するだけで、重要度に応じた診断結果を表示することが可能なクラウド導入診断ツールを作成し、クラウドサービス導入検討（図 4）における利用者と事業者の間のセキュリティ対応状況確認の負荷を圧倒的に軽減することとした。そして、実際のシステム要件により、クラウド導入診断ツールを用いた導入検討を実施し、導入プロセスにおいて、クラウド導入診断ツールの有効性を検証・評価した。検証の結果、代表的な 4 つの心理的不安は低減できると確信した。

図 4.クラウド導入検討の流れ



8．まとめ（提言）

本研究により、利用者が抱えているクラウドサービスに対する心理的な不安は、プロセスを明確にすることで低減できることを確信した。さらに、ツールによりクラウド導入における初期検討負荷の圧倒的な軽減を図れた。このプロセスとツールの活用により自社のクラウド導入スキームを確立し、クラウドに適したシステムから積極的にクラウドサービスの導入に取り組まれることを提言する。