クラウド利用基準整備要領に関する考察の件
Consideration on cloud usage standards

中條正志・マネジメント分科会・情報セキュリティ大学院

Abstract In recent years, as seen in the cloud-by-default advocated by the Japanese government, cloud utilization is expanding. Along with this, incidents due to incorrect settings and internal fraud when using the cloud are also seen here and there. When using the cloud, it is an iron rule to check the demarcation point of responsibility, confirm the security control measures of the vendor, and ensure the responsibility of the user on the user side. There are also some cases where sufficient security measures are not taken. As one of the security measures on the user side, it is an effective measure to use cloud-related guidelines to develop and operate cloud usage standards on the user side. In this paper, we consider the development guidelines for company-specific cloud usage standards based on cloud-related guidelines.

1.研究背景

クラウドサービスのセキュリティ課題
導入が更に進むと考えられるクラウドサービスを安全・安心に利用するためにセキュリティ対策の実施が求められる。（出典）情報セキュリティ白書２０２２ IPA

クラウド整備基準対策の重要性
制度やガイドライン等を活用し、組織がクラウドを利用する目的に見合ったセキュリティ対策を実施していくことが重要である。（出典）情報セキュリティ白書２０２２ IPA

組織事情との適合性の観点
現存する指針やルール(顧客サービスの方針やセキュリティポリシー等)と照らし合わせた上で、運用（出典）クラウドを利用したシステム運用に関するガイダンス NISC

セキュリティ対策を講じる上で企業事情に見合ったクラウド利用基準整備が必要
→**公表されているガイドラインを使って企業固有ガイドラインへ落とし込む要領を整備**

2.整備要領の必要性

各機関が発刊しているガイドラインをそのまま利用するには、以下阻害要因が有、企業実態を踏まえた要領整備が必要

項目	内容
大量の情報	入念な解説党、多くの情報を含むガイドラインを実務で利用するには負荷が高い
利用者組織のポリシー	クラウドサービス利用・提供における適切な設定のためのガイドラインにて、“自社のポリシーへの適合を行う必要がある”と示されている
具体化	内容が例示であったり、基準が明確化されていないことが多いため、企業として評価・判断するための具体化を行う必要がある
独自要素	企業固有の評価・統制項目が必要かも確認する必要がある

3.整備要領提案プロセス

現状分析	規程位置づけ・特定	参照ガイドライン特定 企業特性・要件より分岐		読み解き・落とし込み
課題分析 上記を踏まえた対応方針の策定 関係者洗い出し・特定 既存運用影響分析 関係者との合意／しかるべき意思決定	影響分析担当の選定・確保 企業の規定体系を踏まえ、新設・改訂すべき、対象の特定 ー規定体系がない場合や不足している場合は整備要 ーポリシー、スタンダード、プロシージャーのどこまで整備要か特定	法・規制	監督指針 等	検討体力の見極め、基準改定担当の選定・確保 ガイドラインから、企業規程のどこに落とし込むべきか ーガイドラインと企業規程の紐づけ ーガイドラインを企業規程に落とし込むときの観点・考慮点の明記
		規格	ISO/IEC 271017 ISMAP 等	
		業界	金融であれば FISC安全対策基準	
		国際ガイド	NIST SP800-53 等	
		日本省庁	総務省 クラウドサービス提供における情報セキュリティ対策ガイドライ 等	
		日本団体	IPA クラウドサービス利用の手引き、JIPDEC関連文書 等	
		CSP	AWS Well-Architected 等	

4.今後の研究方針

成果物	手順書、ガイドライン特定フロー等の作成
評価	・提案プロセスを、実例分析を行った企業実例にあてはめて、効果などを評価 ・自己評価だけでなく、セキュリティ関連団体組織メンバーへのアンケート評価も相談・実施予定