SaaS利用者の信頼にこたえるセキュリティ評価フレームワーク

A Security Assessment Framework That Ensures Trust for SaaS Users

対馬 亜矢子・マネジメント分科会・情報セキュリティ大学院大学

1. 研究背景

SaaSの業務利用が増加し、SaaSのセキュリティインシデントが利用者の社会的信用や業務継続に影響する時代となった。多くの場合SaaSを利用するのは、ITシステムの運用管理ではなく本業に注力するためである。ところが現状、SaaS利用者は自社の管理下にないシステムのセキュリティを正しく評価し、監督する責任を負っている。

既存のSaaS評価方法としては下記がある。

- 自社でチェックシートを作成し、契約時に聞き取りを行う
- ISMSやプライバシーマークなど公的認証の有無で評価する
- SaaS提供者の自己評価結果を参照する
- 有償のSaaSセキュリティ評価サービスを利用する

いずれも 正確さ・客観性・即時性 において課題がある。

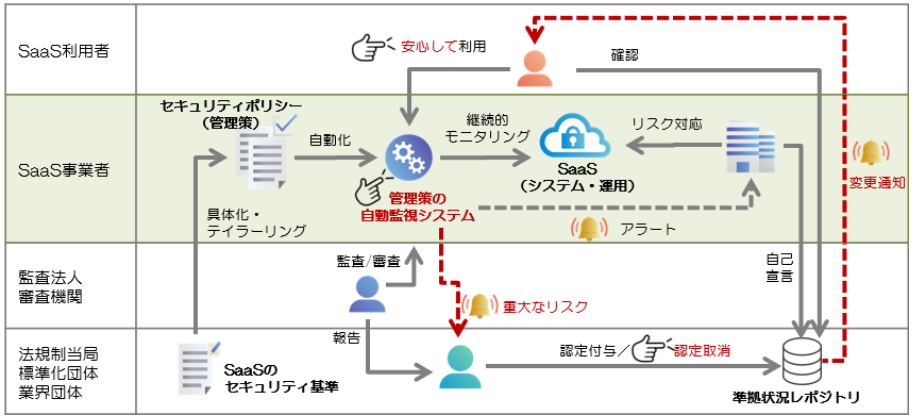
2. 目的

IT・セキュリティの専門知識がない中小企業でも、安心してSaaSを利用できる枠組みの提案

3. 関連制度・技術動向

- CIS Controls: Measures and Metrics
- Cloud Security Alliance：STAR (Security, Trust, Assurance and Risk)
- EU Cloud Certification Scheme、Medinaプロジェクト
- OSCAL (Open Security Controls and Assessment Language)
- NIST SP 800-55：Measurement Guide for Information Security: Volume 1 – Identifying and Selecting Measures
- FedRAMP Continuous Monitoring
- Policy as Code / Compliance as Code

4. 提案内容



5. 期待できる効果

SaaS提供者	ほぼリアルタイムの内部統制に基づく、 効果的なセキュリティリスクマネジメントと情報開示
SaaS利用者	SaaSのセキュリティ基準への遵守状況を、 ほぼリアルタイムで把握できる

6. 今後の計画

技術面

・管理策の自動監視はどこまで可能で、何が課題かを明確にする

社会実装面

・内部統制の自動化を前提とした、監査・審査のあり方の検討