中小SaaS事業者のセキュリティ運用を可視化する透明性フレームワーク CyHACCP

CyHACCP: A Transparency Framework for Visualizing Security Operations in SME SaaS Providers

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

Abstract: The adoption of industry-specific SaaS (Vertical SaaS) is rapidly expanding in Japan. These services are primarily provided by small and medium-sized providers, such as startups, and are mainly utilized by small and medium sized enterprises (SMEs). However, it remains difficult for SME users to independently assess the security of SaaS services. This paper proposes "CyHACCP", a framework designed to enhance the security transparency of SME SaaS by visualizing security operations. Its core automated assessment tool was implemented using Open Policy Agent (OPA) and was confirmed to operate in conjunction with AWS built-in security capabilities, including AWS Security Hub, for vulnerability management and access control configurations. Furthermore, a scenario-based validation demonstrated that SME SaaS providers can improve security transparency by applying CyHACCP in a cost-effective manner. The contribution of this research lies in proposing a practical framework for enhancing transparency in SME SaaS security operations and implementing its core assessment mechanism, thereby demonstrating a realistic approach for the SME SaaS providers.

1. 研究背景と目的

- スタートアップなど中小SaaS事業者が提供する業種特化型SaaS（バーティカルSaaS）の増加
- 人手不足によるデジタル化推進により、中小企業における中小SaaSの利用が拡大

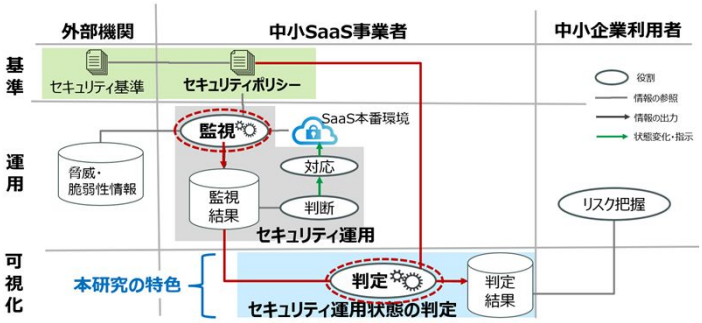
研究目的：IT専門家ではない中小企業の利用者に対する中小SaaSのセキュリティ透明性を向上する

2. 現状の問題点

- SaaSのセキュリティインシデントによる利用者の信用失墜や事業継続への影響
- 中小企業の利用者が、中小SaaSのセキュリティ対策を確認するのは困難（認証制度やチェックシートでの確認は機能しない）
- 中小企業は、中小SaaSのセキュリティについて十分な情報を得られずに利用／インシデントが起きて被害にあうまで問題に気づけない

3. 提案フレームワーク CyHACCP

中小SaaSのセキュリティ運用の透明性を高めるためのフレームワーク

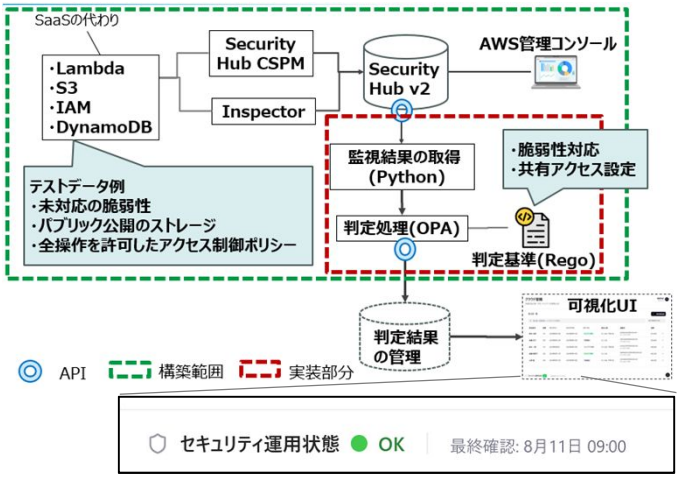


CSPMなどセキュリティ対策の監視結果を，SaaSのセキュリティポリシーに照らしてPolicy as Codeにより判定し，利用者向けに可視化する.

脆弱性対応の判定基準例

No.	管理項目	推奨基準	必須基準
1	脆弱性スキャンツールによる自動監視の実施	—	毎日
2	攻撃コードありの脆弱性の猶予期間	5日以内	21日以内
3	緊急ランクの修正可能な脆弱性の猶予期間	10日以内	31日以内
4	高ランクの修正可能な脆弱性の猶予期間	—	90日以内
5	サポート切れのソフトウェアの使用	0件	—

4. 検証



中核となる自動判定ツールをOpen Policy Agent (OPA)を用いて実装。サーバレス構成のSaaSを想定した検証環境で、脆弱性対応および共有アクセス設定について、判定ツールがAWS標準のセキュリティ監視機能と組み合わせて動作することを確認。中小SaaSがCyHACCPを適用して低コストでセキュリティ透明性を向上できることを，シナリオベースで検証した.

5. 結果

A：中小SaaS事業者にとって	
① 低コスト	○ パブリッククラウド標準機能を利用することで、低コストで運用できる
② 専門家への非依存	○ CyHACCPが提供する判定基準・ツールを利用することで、外部の専門家に依存せず、内部要員で導入・運用できる
B：中小企業利用者にとって	
③ 理解可能	○ 信号色のステータスで、IT・セキュリティ専門知識がなくても理解可能
④ 最新性	○ 監視結果を基にした自動判定により、最新のステータス情報を確認
⑤ 客観性	○ 自動的な判定による客観性のある情報開示 △ 誤検知等を手動で除外する仕組みにより、意図的な不正の余地あり

6. まとめ

- 中小SaaSのセキュリティ運用の透明性を高める**実用的なフレームワークを提案**し，その**中核となる判定ツールの実装**を通じて，中小SaaSに適した現実的なアプローチを提示した.
- 課題：判定基準メトリックスの標準化、可視化UIの見せ方、不正検知の仕組みなど