SaaS サービスのセキュリティ評価とセキュリティ設定の課題とポイント

サイリーグホールディングス株式会社　大越　いづみ
一般社団法人日本クラウドセキュリティアライアンス（CSA ジャパン）　諸角　昌宏

はじめに

本稿は、SaaSの普及に伴い、各企業が直面するセキュリティ評価・設定・運用に関する課題を明らかにし、組織としてどのように対応すべきかについて検討するものである。

SaaSは高い利便性とスピードを提供する一方で、ベンダー依存度が高く、ユーザー側の設定ミスや管理不備による情報漏えいのリスクが顕在化している。特に、Salesforceなどの大規模SaaSにおいて、設定変更や仕様変更に伴う課題が発生しており、「設定を正しく保つこと」自体が難しくなっている。また、このような現実的な問題に直面している企業・組織に対し、セキュリティ評価の考え方、ツール活用の現実解、そして実務者同士の連携による知見共有の重要性について整理し、“自社だけで守る”発想を超えたセキュリティ運用の新たな視座を提示することが求められている。

本稿では、こうした課題に対して、以下の3つの方向性を提示する。

- SaaSセキュリティのリスク構造の可視化と評価の枠組み整備
- SSPM等のツールの適切な活用と運用体制の見直し
- 利用者間の知見を相互補完する「コミュニティ形成」の推進

本稿は、セキュリティ実務者、IT部門責任者、経営層、そして業界横断的な協議体にとって、「SaaSを安全に活用するための戦略と実務をつなぐ手引き」として活用されることを意図している。

1．SaaSセキュリティのリスク構造の可視化と評価の枠組み整備

クラウドセキュリティにおいて、SaaS利用者には以下の2つの大きな責任がある。

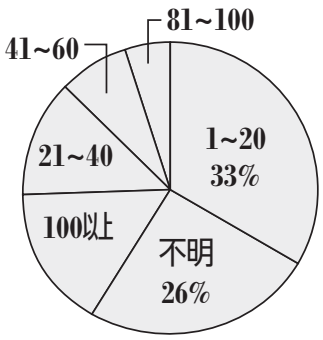
・SaaSサービスのセキュリティをSaaS利用者のセキュリティ要件に基づいて評価し、判断を行う説明責任
・SaaS利用者の責任範囲において、セキュリティ要件を満たすためのセキュリティ対策を自ら行う管理責任あるいは実施責任

まず、最初のSaaSサービスのセキュリティ評価の課題として、「SaaSサービスの利用状況の把握・可視化の課題」と「SaaSサービスのセキュリティ評価方法の課題」について、そのポイントと考慮点について説明する。

①SaaSサービスの利用状況の把握・可視化の課題

SaaSサービス利用においては、部門主導でSaaSを導入するケースが多く、組織あるいはIT部門が、利用しているSaaSの全体を把握できていないケースが多い。「組織で利用しているSaaSサービスの数」というアンケート では、一番多かったのは「1-20」であったが、「不明」が全体の26%を占めていた。これは、組織としてSaaSサービスの利用状況があまり把握できていないことを示している。利用状況が把握できないことによって、不十分なアカウント管理、外部SaaS間の連携におけるデータの流れが不明瞭、インシデント対応の遅れ、コンプライアンス違反などの原因となりうる。

利用しているSaaS クラウドサービスの数の割合



ここでは、これらの問題を掘り下げることはしないが、SaaSサービスの利用状況の把握・可視化の対策の考慮点として以下の2点を上げる。

» SaaS導入・利用に関する明確なポリシー策定、利用者の意識向上トレーニング

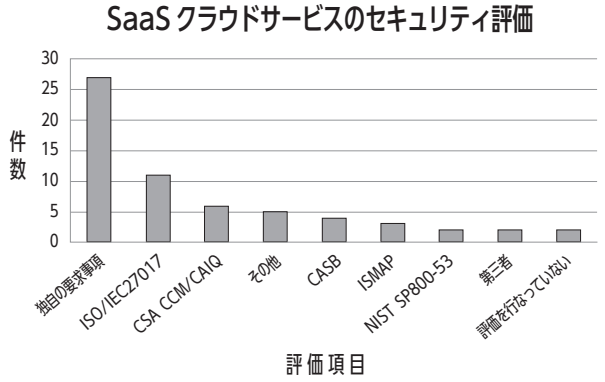
ポリシー策定により、無秩序なSaaS利用を抑制し、データ漏洩・ガバナンス欠如のリスクを回避し、SaaS

の導入基準等に基づくIT部門・セキュリティ部門の管理が可能になる。

» CASB、SSPM等のツールの導入
CASBの導入により未承認SaaSの検出、インターネットトラフィックの監視化が可能になる。また、CASBのDLP機能により、データ分類とDLPポリシー適用が可能になる。また、SSPMによりロール・権限の棚卸しと是正、モニタリングを行うことができる。

②SaaSサービスのセキュリティ評価方法の課題

この課題について、「SaaSのセキュリティ評価を行う際、何らかのフレームワーク（ISO/IEC27017, NIST SP800-53、CSA CCM等）を利用しているか」というアンケートを行った結果が下図で、独自に行っている組織が圧倒的に多いことが分かる。独自にチェックリストを作成し、クラウドプロバイダに確認する方法では、チェックリストを作成するために非常に大きな時間と工数が必要であるとともにクラウドセキュリティに精通した専門家が必要になるという課題がある。



セキュリティ評価を行う際に考えられる方法として、以下の3つについてその有効性と課題を上げる。

» フレームワークをベースにしたチェックリストの作成
チェックリストの作成において、フレームワーク（ISO/IEC27017、NIST SP800-53、CSA CCM等）を利用する。フレームワークを用いることで一般的な要求事項がカバーされる。そこでカバーされない業界あるいは組織固有の要求事項を個別にチェックリスト化することで効率的なチェックリストの作成を行うことができる。

» サードベンダーを利用する方法
VRM、TPRMと呼ばれる方法で、コンプライアンス的な判断を行うには有効と考えられる。課題としてはクラウド利用者のリスク要件をどこまで取り込めるかを検討する必要がある。

» CASBが提供しているセキュリティスコアを利用する方法
CASBが提供しているセキュリティスコアをそのまま採用してSaaSサービスを利用するかどうかの判断を行う方法であり、既にCASBを利用している場合には非常に分かりやすく容易に利用できる方法である。ただし、あくまで一般的な評価であり、クラウド利用者ごとのリスクアセスメントを考慮したスコアではないことは注意する必要がある。

なお、セキュリティ評価を、SaaSの利用形態に基づいてメリハリをつけて行うことも有効である。組織全体でインフラ的に使われるSaaS（Box、Slack、Salesforce等）については、リスクベースのアプローチに基づいた詳細なセキュリティ評価を行う。部門からの利用要求に基づいて利用するSaaSについては、一般的な評価基準（IPAの「中小企業のためのクラウドサービス安全利用の手引き」など）に基づいて評価し、最低限（ベースライン）のセキュリティ評価を行うことで、効率的な評価を行うことができる。

また、SaaSセキュリティの評価以前に情報の分類が課題である。情報の分類がしっかりと行われることにより、IT/セキュリティ部門はCASB,DLP等を使って容易に監視することができ、セキュリティ評価に基づいた運用が行われているかどうかを監視することができる。

2. SSPM等のツールの適切な活用と運用体制の見直し

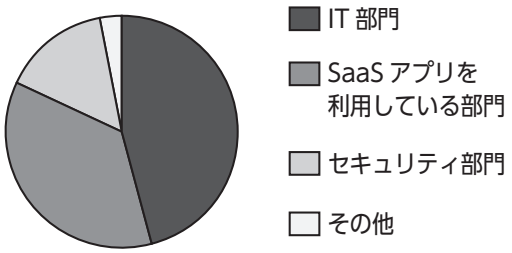
クラウド利用者として、セキュリティ設定の課題は主に以下の2点である。

- 設定の可視性の課題
- アイデンティティ管理の課題

①設定の可視性の課題

SaaSサービスのセキュリティ設定を行っている担当者についてのアンケートに対して、一番多いのはIT部門で46%、その次がSaaSを利用している担当部署で36%であり、担当部署がセキュリティ設定を行っているところが多いことがわかる。このことは、ビジネスチーム（部門）に柔軟性を提供する一方で、セキュリティの盲点を生み出すことに繋がっている。

セキュリティ設定を担当する部署



これにより想定される問題は以下の点である。

» 不十分な特権とアクセス管理
最小特権アクセスポリシーが効果的に実施されていなかったり、データへの過剰なAPIアクセスを許可していたりすることにより、機密データが外部に過剰に公開されるという問題が発生する。また、従業員が機密データを未認可なSaaSアプリケーションにアップロードしてしまうということも発生する。

» 従業員がセキュリティ部門の関与なしにSaaSアプリケーションにサインアップ
IT/セキュリティ部門以外が SaaS 管理を実施するため、どのようなアプリケーションが使用され、どのように設定され、機密データがどこに保存されているのかを組織として把握できない。ガバナンスへの一元的なアプローチがないため、セキュリティポリシーが矛盾して適用され、設定ミスのリスクやセキュリティインシデントへの対応の遅れが生じることになる。また、明確なオーナーシップがないため、ポリシーの実施にギャップを生じることとなる。

②アイデンティティ管理の課題

SaaSのアイデンティティ管理として、以下の2点を考える必要がある。

» 人的アイデンティティ管理
» 人間以外のアイデンティティ管理
（NHI: Non-Human Identity）

人的アイデンティティの最大の課題は特権管理である。一貫した特権付与が行われないと、ユーザーが必要以上の権限を保持する可能性があり、データ漏洩や内部脅威のリスクが高まる。また、複数のSaaSアプリケーションにまたがるユーザーアクセスの管理は、アイデンティティ管理の不備を利用したSaaSアプリケーション間のラテラルムーブメントを引き起こす可能性がある。

人間以外のアイデンティティは、APIベースの接続、OAuthトークン、サービスアカウントなどで、特権の行使、アイデンティティの乱立が起こる可能性がある。また、一度設定されると放置され、監視されないことが多いということも言える。

さて、本題であるツールの適切な活用と運用体制の見直しとして、実際にSSPMを利用している管理者からみた有効性および課題についてまとめる。

①SSPM

SSPMの利点をまとめると以下になる。

» 設定の可視化
» 設定値の取得、設定値の判断の自動化
» 素早い検知が可能（SSPMの検知機能）
» SaaSの機能追加等に対する確認が可能（SSPMのアラート機能）

半面、以下のような3つの課題があることも認識しておく必要がある。

» SSPMがサポートしていないSaaSへの対応
特に、日本のSaaSへの対応が低いことが挙げられる。これは、SSPMがSaaSサービス側のAPIと連

携するため、SaaSサービス側が対応できていないケースが上げられる。

» SSPMのライセンス費用の問題
SSPMのライセンス体系では、費用が掛かりすぎる問題がある。したがって、全社展開する主要なSaaSをSSPMで管理し、部門だけが使用しているSaaSは手動で管理するというようなメリハリを持った利用が必要となる。

» SSPMの指摘に対する対応
SSPMの指摘に対してすべて修正するのはなかなか難しい。影響が出そうなものに限定した対応を行う等の対策が必要である。

3. 利用者間コミュニティの形成の重要性

SaaSのセキュリティ評価基準の策定や設定項目の管理、ツールの活用といった課題に対し、各組織が個別に手探りで取り組んでいるのが実情である。特に、設定ミスや設定変更による情報漏えいリスクの顕在化は、単に技術的な課題というよりも、「孤立した運用体制」に起因する側面が大きい。こうした背景から、実務知見を組織横断で共有・補完し合うための「利用者間コミュニティ」の形成が、今まさに強く求められている。

①現場での“知の孤立”が引き起こすリスク

多くの企業がSaaSを導入する一方で、これらの設定管理や脆弱性把握の実務は現場任せになりがちである。特にSaaS特有の設定体系は複雑かつ動的であり、「何をチェックすべきか」「安全な初期設定とは何か」すら、ベンダーからの情報提供では不十分なことが多い。その結果、設定ミスが放置され、組織の機密情報が意図せず公開されてしまう事例が相次いでいる。こうした課題を自力で解決するには、相応の人材・知識・ツールが必要だが、全てを自組織内でまかなうのは現実的ではない。

②コミュニティがもたらす３つの価値

こうした状況を打破するためには、利用者同士の知識共有による「知の集約」が鍵となる。利用者間コミュニティには、大きく以下の3つの機能が期待される。

» ナレッジと経験の共有
まず、各社で行っているSaaSのセキュリティ評価、SSPMやCASBの活用方法、設定管理の実践知、例えば、ある企業での設定ミスやその検出プロセスは、他社にとっても極めて有用な予防情報となる。また、評価基準やチェックリストを公開・共有することで、自社の対応状況を客観的に見直す材料にもなり、実践的なベンチマーク形成にもつながる。

» インシデント対応力の向上
次に、SaaSベンダーの仕様変更や新たな脆弱性に関する情報は、利用者間での早期共有が極めて重要である。特にゼロデイ脆弱性や意図しないデフォルト設定の変更などは、公式発表だけではカバーしきれないタイムリーな対応が求められる。利用者間での速報的な情報共有や対応方法のディスカッションは、個社では得られない即応力と安心感を生み出す。まさに、“実運用に根差したセキュリティレーダー”としての役割が期待される。

» 人材育成と横断的ネットワークの形成
SaaSセキュリティは、技術とツールだけでは守り切れない。情報の共有、実践知識の蓄積が早期対応の面において有効である。そのために「利用者間コミュニティ」は、組織の枠を越えてセキュリティ力を高めるための実効性の高い解決手段のひとつである。コミュニティでは、実務者同士の交流や勉強会を通じて、実践的なノウハウを学ぶ場を提供できる。また、自社とは異なる業界・業種の取り組みを知ることで、自らの立ち位置を客観視し、戦略や投資の優先順位を再考する機会にもなる。こうした横断的なネットワークは、将来的にセキュリティ標準や業界横断ルールの形成にも寄与し得る。

③既存の取り組みと自発的な活動の重要性

すでに国内でも、CSAジャパンなどを中心に、SaaSセキュリティ評価や設定管理に関する研究会やワーキンググループが活動を開始している。また、サイリーグとCSAジャパンは、SaaSユーザー企業の実務者を対象とするラウンドテーブルを開催したところ、同じような立場にある実務者同士の非公式な情報交換会は有意義な取り組みであるとして好評であった。さらに、継続的に情報交換できるコミュニティが欲しいという意見も上げられた。

一方で、コミュニティは「用意されるもの」ではなく、メンバーが「参加し、共に築いていくもの」である。各組織においても、社内のSaaS管理者やセキュリティ担当者を横串でつなぎ、自組織内コミュニティの形成から始めることが望ましい。並行して、外部との知見交換に開かれた姿勢を持つことが、結果として組織全体のセキュリティレベル向上につながる。

4. まとめ

SaaSセキュリティは、「導入すれば安心」なものではない。むしろその運用と継続的な設定管理こそが、最大の挑戦の一つとなる。従来のセキュリティ管理では想定されなかった「設定の透明性の欠如」「不十分な仕様変更の通知」「責任の分散化」といった課題は、SaaS特有のものとして新たなアプローチが求められている。

本稿で述べたように、SSPMやCASBなどのツール活用によって技術的なカバレッジを補完することが望ましい。一方で、「設定を正しく保つ文化と仕組み」そのものをどう構築するか。これが今後の焦点となる。組織は「個別最適」から「集合知による最適解」への移行を強く意識しなければならない。セキュリティ対策は、もはや“競争”の対象ではなく、“連携”と“共創”の領域へと進化しつつある。

本稿が、SaaSセキュリティの課題に向き合う実務者・管理者・経営層の対話の一助となることを願ってやまない。

i) アンケートは、2025/2/7～2025/3/20、主に日本クラウドセキュリティアライアンスの会員で実際にSaaSのセキュリティ評価や設定を担当されている方に実施したもので、回答数は39件である。