クラウド利用者のためのSaaS ガバナンスのベストプラクティス

cloud security alliance®

SaaS ワーキンググループの恒久的かつ公式な場所は、https://cloudsecurityalliance.org/research/working-groups/saas-governance/です。

Acknowledgments

Finishing Initiative Leads

Chris Hughes
Tim Bach
Michael Roza
Anthony Smith
Walter Haydock
Andreas Peter
Andrew Luhrmann
James Underwood
Alistair Cockeram
Saan Vandendriessche

Finishing Contributors

Bryan Solari
Sai Honig
Amit Kandpal
Jessica Shouse
Abhishek Vyas

Finishing Reviewers

Jerich Beason
Kapil Bareja
Or Emanuel
Udith Wickramasuriya
Priya Pandey

Initial Leads and Contributors

Akin Akinbosoye
Yao Sing Tao
J.R. Santos
Mickey Law
Vani Murthy
Zeal Somani
Paul Lanois
Michael Roza

CSA Global Staff

Shamun Mahmud

日本語版提供に際しての告知及び注意事項

本書「クラウド利用者のためのSaaSガバナンスのベストプラクティス」は、Cloud Security Alliance (CSA)が公開している「SaaS Governance Best Practices for Cloud Customers」の日本語訳です。本書は、CSAジャパンが、CSAの許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSAジャパンは何らの保証をするものではありません。
この翻訳版は予告なく変更される場合があります。以下の変更履歴(日付、バージョン、変更内容)をご確認ください。

変更履歴

日付	バージョン	変更内容
2022年08月05日	日本語版1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス(CSAジャパン)は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1.　責任の限定
CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。
(1)　本書の内容の真正性、正確性、無誤謬性
(2)　本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3)　本書の内容に基づいて行われた判断や行為がもたらす結果
(4)　本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2.　二次譲渡の制限
本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。
ただし、以下の場合は本項の例外とします。
(1)　本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2)　本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。

(3)　CSAジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4)　転載、再掲、複製の作成と配布等について、CSAジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3.　本書の適切な管理
(1)　本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2)　本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3)　本書をダウンロードした者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4)　本書を印刷した者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4.　原典がある場合の制限事項等
本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5.　その他
その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「クラウド利用者のためのSaaSガバナンスのベストプラクティス 」は、CSAジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

石井　英男, CISSP, CISA, CISM
納本　健太, CISSP-ISSMP, CCSP, CIA
小野　貴博
木村　チエ
昆　資之
鈴木　伸
永田　真弓, CISSP, CISA,
西　誉
根塚　昭憲
羽田　昌弘, CISSP, CCSP
松浦　一郎, CISSP, CISM, CDPSE
松崎　祥三
諸角　昌宏
山口　弘行
渡邉　浩一郎, CISSP, CISA, CEH

目次

1. はじめに

組織が2-3社のIaaSプロバイダを利用する傾向がある一方で、数十から数百のSaaSプロバイダを利用していることが多いという現実があるにもかかわらず、クラウドセキュリティの文脈では、ほとんどの場合、IaaS（Infrastructure as a Service）とPaaS（Platform as a Service）環境のセキュリティに焦点が当てられています。クラウド利用者のためのSaaSガバナンスのベストプラクティス は、SaaS環境における基礎的なガバナンス実践のための、基準となるセットです。 評価、採用、使用、解約など、SaaSライフサイクルのすべての段階でリスクを列挙し、考察します。

組織は、SaaSベースのアプリケーションやソリューションを採用していく中で、従来の組織のサイバーセキュリティのいくつかの領域に、この新しい運用モデルを反映して更新する必要があります。

組織内のポリシーは、サービスレベル合意書、セキュリティやプライバシーの要件、運用への影響など、重要な項目を反映したものに更新する必要があります。組織のセキュリティ活動の運用は、責任や、モバイルデバイスと従業員のリモートワークのように関連性のある課題によっても、影響を受けます。情報は資産であり、外部のサービスプロバイダが提供するSaaSにおいて、情報の分類、ラベル付け、保管の要件について考慮しなければなりません。 SaaSプロバイダは責任共有モデルにおいて多くの責任を負っていますが、SaaS利用者はデータガバナンスとアクセスコントロールに関して依然として大きな責任を負っています。これは、特にゼロトラストアーキテクチャにおいて、誰がどのデータに、どのレベルの権限で、どのような状況下でアクセスできるかを確実にしなければならないことを意味します。

組織には依然として、暗号鍵の管理、ならびに脆弱性管理、バックアップおよびストレージといった運用活動に関して決定すべき重要事項が残っています。組織は、SaaSプロバイダをサードパーティーリスク管理プログラムの一部として考慮し、インシデント対応や事業継続の計画やプロセスを適宜更新していく必要があります。このことは、SaaSが、リモートワークパラダイムにおいて、事業継続性の観点から重要な機能を果たすことが多くなってきているため、ますます間違いのないこととなってきています。
責任が共有されているとしても、組織は、ステークホルダーやレピュテーションを守り、潜在的な法的影響を回避するために、コンプライアンスや規制の要件を満たさなければなりません。
SaaS環境は、提供者と利用者の間に責任の共有を導入することで、最終的に、組織におけるサイバーセキュリティの取り扱い方法に変化をもたらします。 適切な調整を怠ると、機密データの開示、収益の損失、顧客の信頼、規制への影響など、壊滅的な結果を招く可能性があります。

1.1 スコープ

本書は、以下の点をカバーします。

- SaaS環境内のデータを保護するためのSaaSガバナンスのベストプラクティスの基準セットを提供します
- SaaSの採用・使用ライフサイクルに応じたリスクを列挙・考察しています
- SaaSの利用者視点での潜在的な緩和策を提供します

1.2 想定読者

- SaaS利用者
- SaaSプロバイダ
- SaaSセキュリティソリューションプロバイダ
- クラウドセキュリティ専門家
- 法務部門
- サイバーセキュリティエグゼクティブ
- ITエグゼクティブ
- リスク管理者
- IT監査人やコンプライアンス部門
- サードパーティーリスク管理者

2. 概要

SaaS（Software as a Service）の利用者は、SaaSサービスの使用によって生じる情報セキュリティリスクを評価し、軽減する必要があります。この文書は、SaaSを「クラウドインフラ上で動作するプロバイダのアプリケーションを使用することによって利用者に提供される機能 」と定義しているNIST 800-145の文脈で、SaaSについて論じています。 この文脈において、利用者は特定のコンフィギュレーション設定を除き、クラウドインフラ、オペレーティングシステム、関連ストレージ、あるいは個々のアプリケーションの管理または制御は行いません。

クラウドの導入とセキュリティの領域は進化し続けていますが、SaaSのガバナンスとセキュリティに関するガイダンスはあまり多くありません。しかし、重要なビジネスプロセスと機能を強化するために、そして、しばしば機密データをSaaS環境に保存するために、組織内の様々な部署によって折に触れSaaSサービスの利用が増加（シャドーIT）しているのが現実です。

2.1 アプローチ

SaaSでは、セキュリティガバナンスの考え方が異なります。他の責任共有フレームワーク（IaaSなど）のガバナンスと類似している部分もありますが、SaaSの配備と管理の性質上、独自のアプローチが必要とされます。SaaSの適切なセキュリティとガバナンスのデューデリジェンスは、SaaSアプリケーションの用途と機能を理解するという高いレベルから始め、どのような種類のデータがシステムに保存され、誰がアクセスするのかといった細部にまで踏み込んでいく必要があります。

SaaS アプリケーションの利用を適切に管理するという独特な複雑さと、導入される可能性のある無数のSaaSアプリケーションを考慮すると、組織はまず、組織のセキュリティ、ビジネス、および規制のニーズに合ったフレームワーク（NIST CSF など）を探す必要があります。このフレームワークによって、セキュリティアーキテクチャを構成する人、プロセス、および技術が形成されます。

NIST CSFのような広く採用されているセキュリティフレームワークに従って、本書のベストプラクティスや推奨事項を組み合わせることで、組織はSaaSガバナンスとセキュリティプロセスを確立し、SaaS使用に伴うリスクを軽減することができます。

2.2 構造

本書では、SaaSのセキュリティに必要な3つの要素「プロセス」「プラットフォーム」「アプリケーション」を定義しています。SaaSの統合セキュリティは、プロセスセキュリティ、プラットフォームセキュリティ、アプリケーションセキュリティを統合した戦略で実現することができます。

プロセスセキュリティは、プロセスの入力と出力が容易に損なわれないように、手続き上の活動の完全性を保護します。組織のプロセスの一貫性を確保するための方針や手順などを含む、管理的な側面を持ちます。

プラットフォームセキュリティは、プラットフォームセキュリティの強度、SaaSサービスの潜在的な依存関係を扱います。この中には、SaaSのインフラ、オペレーティングシステム、およびそれらにおける潜在的なサプライヤーも含まれます。

アプリケーションセキュリティは、SaaSアプリケーション自体のセキュリティを扱います。SaaSアプリケーションは、悪用可能な脆弱性を含まず、組織やベンダーのセキュリティベストプラクティスやコンプライアンス要件に沿った強固な構成を実装して初めて、安全性を維持することができます。

SaaSモデルでは、コントロールは制限され、可視性は主にプロセスとアプリケーションのセキュリティコンポーネントに制限されます。SaaS利用者は、SaaSアプリケーションのプラットフォームセキュリティコンポーネントや基盤となるサプライチェーンを制御することはできません。このような現実から、SaaS利用者は、組織内で健全なプロセスセキュリティを確保し、アプリケーションレベルのセキュリティ管理を確実に実施する必要があることを強調しています。

セクター固有のセキュリティ管理は、一般的に、プライバシー、政府、または財務のコンプライアンスを満たすために使用されます。例えば、FedRAMP、NIST 800-53、HIPAA、PCI-DSSなどです。これらの要件は、多くの場合、SaaSの3つのセキュリティ領域に対して横断的に適用される、垂直的な着眼点を持つものです。

2.3 ライフサイクルの考慮事項

適切に管理されている場合、企業環境におけるSaaSアプリケーションの採用と使用は、一般的に、評価、採用、使用の3つの主要なライフサイクルに沿って行われます。これらのライフサイクルの一般的なパターンを以下に説明します。

ただし、SaaSアプリケーションの監視が遅れている多くの組織では、SaaSアプリケーションの採用が有機的に拡大している可能性が高いことに留意することが重要となります。SaaSのセキュリティとガバナンスプログラムが、SaaSの普及後に導入されるこのような組織においては、使用のライフサイクルとの関連性が最も重要になります。

2.3.1 評価ライフサイクル

評価ライフサイクルは、SaaSアプリケーションによって解決される可能性のあるビジネスニーズを特定することから始まり、これは調達の前に行われます。多くの組織では、これは事業部門で行われ、中央の調達組織が関与する場合もあればしない場合もあります。評価ライフサイクルは、通常4つのステップで構成されています。

- 検討中のユースケースにおいて、ユーザーが既に活用しているサービスの把握
- 市場調査
- パイロット版での試行
- 購買決定

組織で購入が決定された場合、SaaSアプリケーションの配備が開始され、以下に示す採用ライフサイクルが開始されます。評価フェーズにおいては、関連するセキュリティ及びコンプライアンス組織の代表者の参加は理想的ですが、採用フェーズではそのような代表者の関与が非常に重要となります。組織がSaaSセキュリティとガバナンスのプログラムを構築する際、これらの組織的な「関所」が、セキュリティチームにとってSaaSライフサイクルの重要な統合ポイントになります。

2.3.2 採用ライフサイクル

SaaS採用ライフサイクルは、多くの組織で一貫しており、SaaSアプリケーションが初期形態で調達された時点（時には拡張パイロットプログラム）から、本格的な展開と使用量の増加、そして終了と廃棄まで関係します。

採用ライフサイクルの長さは様々で、大規模でビジネスに不可欠なSaaSアプリケーションの場合、現実的には永続的ですが、一般的には以下の4つのステップで構成されています。

- **評価：**評価段階では、クラウド利用者は利用するSaaSアプリケーションの候補を評価します。これは通常、ビジネスニーズを満たす特徴、機能、能力を調査するためのパイロットまたは概念実証の活動を実施します。
- **採用：**採用段階では、クラウド利用者が評価したSaaSを正式に採用し、パイロット版や概念実証版から正式版への移行を実施します。場合により、より機密性の高いデータをSaaSアプリケーションに移行し、さらにビジネスユーザ部門に展開し、利用を開始します。
- **日常的な使用・拡張：**日常的な使用・拡張段階では、継続してクラウドを利用します。クラウド利用者は、使用に関する標準的な業務手順を設定し、SaaSアプリケーションの様々なビジネス機能を日常的に使用します。
- **終了：**終了段階では、クラウド利用者がSaaS利用の終了を決定します。コストやセキュリティ、あるいはビジネスニーズに合わなくなった場合などの様々な理由により、クラウド利用者は、SaaSアプリケーションの使用を停止し、機密データやアカウントなどの削減を実施します。

2.3.3 使用ライフサイクル

SaaS使用ライフサイクルは、日常的な運用リスクや最小権限、アイデンティティとアクセス管理などのセキュリティ上の懸念事項から保護する活動を実施します。

SaaS使用ライフサイクルは、以下の4つのステップで構成されます。

- **適格性：**この人または人ではないこのエンティティがこのサービスを使用するユーザーとして適格ですか？
- **プロビジョニング：**この人をサービスに追加するには何が必要で、どのような権限が必要ですか？
- **モニタリング：**その人は、利用者である組織が期待する使い方と一致したパターンを文書化して使っていますか？
- **デプロビジョニング：**どのようにこの人をサービスから外しますか？

SaaS使用ライフサイクルは、クラウドを使用する組織がCSPとSaaSサービスを使用する場合に必要な実施事項を明確化しています。

SaaS使用ライフサイクルを全体的に理解し、監視することが重要となります。ライフサイクルのうち一つの局面、例えば使用開始に全力を集中させてしまうことはありがちなことですが、そうすることによりビジネス目標をより簡単に、より早く達成することができるわけではありません。

3. 情報セキュリティポリシー

SaaS利用者は、SaaSのセキュリティ戦略を策定し、その戦略を反映したセキュリティアーキテクチャを構築する必要があります。セキュリティアーキテクチャは、SaaSアプリケーションの配備と保守を安全に実施するためのセキュリティ要件を実装する必要があります。

3.1 情報セキュリティに関するポリシー

SaaSサービスの評価、採用、使用、終了を管理するためのポリシーを策定する必要があります。上記の一般的なSaaSのライフサイクルの説明を参照し、ライフサイクルの各段階において、包括的なポリシーと評価管理策を実施していることを確認します。

3.1.1 評価

評価の決定において、エンタープライズアーキテクチャの要件とプロセスによって評価される必要があります。環境の全体的なエンタープライズアーキテクチャ（製品、サービス、ツール、およびそれらで解決する要求事項の評価）を対象とする必要があります。評価の結果により、製品、サービス、ツールの無駄な重複を防ぐことができます。

最初に、現在のエンタープライズアーキテクチャで利用できない要求事項を特定し、続いて製品、サービス、ツールの評価を実施します。

SaaSサービスを初期評価する場合、通常、ビジネス、法務、セキュリティのステークホルダーがクラウド利用のリスクを理解し、実施することになります。評価の重要要素は、「使用するSaaSサービスが、自組織のリスクプロファイルおよびエンタープライズアーキテクチャに潜在的に適合しているか」を評価することです。

3.1.1.1 許容リスクの決定

SaaSサービスを評価する場合、最初にサービス利用時に発生するリスク内容とリスク選好により評価する必要があります。SaaSアプリケーションは、プライベート、ハイブリッド、またはパブリッククラウド環境に実装され、対象となるアプリケーションはアプリケーションレベルの専用または共有リソース（シングルインスタンス、マルチテナント）で提供されます。利用する全てのクラウド製品、サービス、ツールに対して、クラウドを利用する上で定義される責任共有モデルを理解する必要があります。

情報セキュリティ管理に関するアプローチであるISO/IEC 27001では、情報セキュリティ管理のためにリスクマネジメント手法を使用することを提唱しています。SaaS利用者は、最初にSaaS サービス利用時に組織が許容可能なリスクを決定し、評価段階の基本水準とする必要があります。リスクマネジメント手法は、国際的なリスクマネジメント規格であるISO31000をはじめ、さまざまな方法があります。

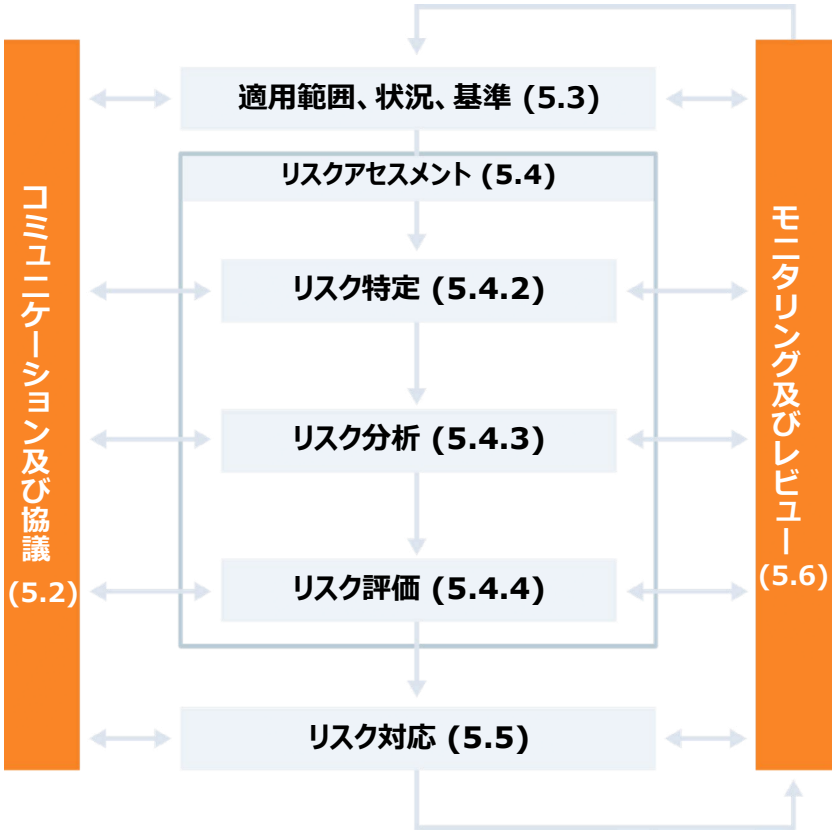

図1. ISOリスクマネジメントプロセス、第5項。プロセス

組織が規定するリスクプロファイルを理解した上で、SaaS利用者は、組織のリスクプロファイルに対するSaaSサービスの適合可能性を判断することが可能となります。

SaaSサービスのリスクプロファイルを決定する１つの方法は、SaaSサービスの利用状況を把握・整理して決定する方法となります。

- データ
  - 何のデータがビジネスプロセスにおいて保存されるか、またはSaaSアプリケーションにさらされるかを確認します。
  - SaaSアプリケーションに保存されているデータの機密性や完全性が損なわれる場合、ビジネスにとって直接的なコスト（影響を受ける個人への通知コスト、株価下落による株主へのコスト、競合他社サービスへの大量の利用者流出、利益損失）、間接的コスト（風評被害や将来の売上の損失、サイバー保険コストの増加、主要スタッフの雇用契約終了）、隠れコスト（対応のためのスタッフの配置転換コスト、侵入ポイントのセキュリティ強化コスト）の影響内容を確認します。
- プロセス
  - SaaSサービスを利用する場合の基幹となる重要なビジネスプロセスに対する影響内容を確認します。
  - SaaSサービスを利用する場合の組織のポリシー及びプロセスの見直しなどの影響内容を確認します。
- 要求事項
  - SaaSサービスを利用する場合に関連するビジネス要件、法律、規制を確認します。

この段階で、以下の評価項目についてSaaS利用者のリスクプロファイルに対する影響内容を確認する必要があります。

- SaaSプロバイダ
- SaaSサービス
- SaaSプロバイダのサプライヤー
- SaaSサービスの利用状況
- クラウド使用のリスクを軽減するため、SaaSプロバイダに対して継続的な監視とポスチャ管理を実施するSaaS利用者の対応能力

最も一般的なリスクプロファイリングの方法は、伝統的な情報のCIA分類となります。

- 機密性
- 完全性
- 可用性

CIA分類は、アプリケーションやデータベースをクラウド利用者の要件に応じてリスク評価を実施します。

クラウド環境にリスクとなる脅威が明確になる場合、SaaS アプリケーションに発生するリスク値の計算を実施することが可能となります。

多様なリスク値を計算する方法から最適な方法を選定し、組織の要求事項と業種の種類に従いリスクプロファイリングのフレームワークを構築する必要があります。

SaaS利用者がCSPにリスク対応を移管する場合、CSPにSaaS利用者としての**説明責任を移管したことにはならない**ことに留意する必要があります。SaaS利用者は、SaaSサービスを採用するリスクを受け入れる責任がリスクオーナーにあることを常に念頭に置く必要があります。CSPとクラウド利用者の間で責任分界点を明文化するサービスレベル合意書（SLA）などの契約を締結しますが、最終的にリスクに対処するのはクラウド利用者となります。

3.1.1.2 セキュリティとプライバシーに関する要件

クラウドサービス利用者は、最初にベースラインとなるリスクレベルを確立し、セキュリティとプライバシーのデューデリジェンスプロセスを実施します。クラウドサービス利用者は、一般的にCSPに評価アンケートやRFI（Request for Information）を送付し、記入・回答を依頼する方法を実施します。

依頼するアンケート等は、クラウド利用者がCSPに求める内部セキュリティ管理について質問する内容であり、通常、セキュリティとプライバシーに関する規制要件の順守状況を確認する内容となります。

クラウド利用者がSaaS プロバイダのセキュリティ能力および現行の対処方法を確認する場合、CSPが実施するCSA STAR Consensus Assessment Initiative Questionnaireや、第三者評価（例えば SOC2 / FedRAMP）などの自己評価制度の内容を効率的に利用することができます。

クラウド利用者は、自己評価や第三者機関の報告内容から、クラウドプロバイダによる個人情報の利用や開示、あるいは個人情報の利用先を確認し、更に、クラウドプロバイダが情報を自社で使用するのか、第三者に開示するのか（例えば、第三者の広告主に対する開示など）を確認することができます。

また、データ主権に関する要件がある場合もあるため、データの所在についても注意が必要です。

評価される第三者評価の主なカテゴリには、以下のようなものがあります：

- 認証・規格
- データ保護
- アクセス制御
- 監査可能性
- 災害復旧と事業継続性
- 法律とプライバシー
- 脆弱性とエクスプロイト

3.1.1.3 要件の伝達

これらのアンケートやレポートの回答によって、利用者はリスク評価をさらに精緻化し、クラウド取引の契約フェーズに反映させることができます。リスク評価とデューデリジェンスプロセスを強化するため、またサプライヤー管理の一環として、多くのクラウド利用者がデータセキュリティとプライバシーの標準的な一覧や条項を作成し、クラウド契約に含めています。

これらの一覧や条項の目的は多岐にわたり、重大な結果をもたらす可能性があります。一つの目的は、特定の地域でデータを維持するなどの規制問題に対処することです。もう一つは、クラウドベンダーに合理的なセキュリティ基準を守らせる仕組みを作ることです。これらの一覧や条項は、インシデント対応義務を定め、クラウドプロバイダに起因するデータ侵害やプライバシー侵害に伴う損失のリスクを移転することもできます。また、データ漏洩などの問題に、指定された時間内、指定された方法で対応するように求めたり、監査権や定期的なモニタリングおよび統制活動を行う権利が含まれることもあります。

さらに、CSPと利用者の間での契約が執行される場所における、またはその契約に適用される、関連する裁判管轄および規制の枠組みを理解することが不可欠です。例として、従業員または利用者のPIIを保存または処理するためのSaaSプラットフォームを探していて、GDPRが適用される場合、CSPがEU/EEA地域または適切な保護を提供する国にデータを保存するかどうかを確認する必要がある可能性があります。そうでない場合は、データが保存される国において適用される法的枠組みを確認し、並びにCSPが妥当な保護を備えていること及び欧州連合司法裁判所（CJEU）のSchrems II判決に基づき、データを保護するための補完的な技術的管理策を備えていることを確認する必要があります。

全体としての目標は、契約上、クラウドプロバイダとシームレスな関係を築き、利用者のリスクを可能な限り低減することを試みることです。

ベンダー管理プログラムの契約プロセスは、クラウドプロバイダとの交渉において、特定の条件に対する「フォールバック」ポジションを利用者があらかじめ設定できるように、さらに洗練されることもあります。これには、関係を終了すべきと判断した場合のデータなどの移管方法（例：ベンダーロックインの防止）が含まれる場合があります。これらの条件の交渉には、利用者の法務チームとセキュリティチームの両方が関与することも珍しくありません。

3.1.1.4 内部統制

利用者は、SaaSのセキュリティ戦略を策定し、その戦略を反映したセキュリティアーキテクチャを構築することが望まれます。SaaSの利用者は、クラウド責任共有モデルのうち、利用者が責任を負う部分に留意するべきです。つまり、SaaSプラットフォームの安全な設定・管理・利用について、設計された範囲内で最終的な責任を負うのは、SaaSプロバイダではなく、SaaS利用者であるということです。

SaaSのセキュリティ戦略を策定する上で、脅威のモデリングと脅威のプロファイリングは重要なポイントです。クラウドセキュリティアライアンスが発表したクラウド脅威モデリングは、「脅威モデリングのセキュリティ目標の特定、評価範囲の設定、システムの分解、脅威の特定、設計上の脆弱性の特定、緩和策および管理策の策定、行動喚起の伝達に役立つ重要な指針を提供する」ことを目的に発行されたものです。

テクノロジーの種類がクラウドであってもそれ以外であっても同様に、SaaSプラットフォームを使用するための効果的なリスク管理とセキュリティ管理には、SaaS利用者がこのプロセスの前半で決定したSaaSアプリケーションのリスクレベルと分類に適した多方面のセキュリティ戦略を導入することが求められます。この戦略には、次のような要素が含まれるでしょう。

- SaaSプラットフォームで適用可能な、適切なクラウドサービス利用者関連のセキュリティコントロールと構成（SSO、MFA、ロール割り当て、チーム/グループ分離、ログのエクスポートまたはセキュリティ監視ソリューションとの統合、IP制限など）の理解と採用
- SaaSの利用状況・妥当性の定期的な検証
- SaaSアプリケーションまたはプラットフォームの外で管理または展開されるビジネスロジックまたはプロセスに関するペネトレーションテスト
- SaaSアプリケーションの構成と、組織固有の承認された/期待される構成との比較による、継続的なセキュリティポスチャの監視
- SaaSアプリケーションによって生成される監査、イベント、その他の変更/活動ログの、理想的にはこれらのログを他のSaaSおよび非SaaSアプリケーションと相関させることができる環境での継続的な監視
- SaaSアプリケーションの重要なデータやプロセスへのアクセスの継続的な監視

3.1.1.5 サービス条件

強固なインシデント対応、およびセキュリティやフォレンジックの評価権について交渉していないこともまたリスクとなり得ます。

SaaSプロバイダが利用者の情報に影響を与える侵害を受けても、侵害の通知を行い、修復を行い、協力する契約上の義務を負わない場合、SaaS利用者は自らの法的リスクを軽減し、規制義務を遵守することができない可能性があります。地域によって法律や通知義務が異なる場合があるため、調達・契約フェーズでサイバー専門の弁護士を確保することが重要です。

検討すべき契約上のコントロール。

- サービスレベル管理
  - サービスプロバイダのSLAと組織のSLA要件との対比（リソースやサポートの見地を考慮する必要があります）
  - 事業継続の保証：RPO、RTOと組織のMTDとの対比
  - インシデント対応とエスカレーション
- バックアップの可用性
- 法的な問題
  - 法律および規制の要件
  - CSPとSaaSサービスの裁判管轄権、法的要求事項
  - 損害補償：裁判管轄の移転、M&A
- 通知：セキュリティ、プライバシー、コンプライアンスの変更、およびイベント
- 解約の権利と手続き
  - データのポータビリティ（他のプラットフォームに移行する場合、データのエクスポートオプションを考慮する必要があります）
  - データの削除、スケジュール、削除が完了した場合の書面による通知
  - 業務委託契約を終了する場合の出口戦略

3.1.1.6 影響されるデータ

クラウドコンピューティングへの移行がもたらす大きなリスクの一つは、クラウドに転送され、ネットワークの可用性がクラウドに委託されたデータに対する絶対的なコントロールが失われることです。

例えば、より従来型のIT環境では、組織は自らのシステムが、適用される規制や標準に準拠するように評価および調整する能力を持っています。これには、組織やその顧客の所在地に基づくデータ所在地に関する要件が含まれる場合があります。

多くのSaaSプロバイダは、複数の裁判管轄に所在するサービスとしてのインフラストラクチャプロバイダを使用しているため、これらの要件を考慮せずにSaaSサービスを使用すると、コンプライアンスに関するリスクが増大する可能性があります。

SaaSの利用者は、以下の質問に答えることができるはずです。

- SaaSプロバイダは、どのような裁判管轄で運営されていますか？
- どのような規制要件が適用されますか？
- SaaSサービスにはどのようなデータが転送されるのでしょうか？
- SaaSサービスではどのようなデータにアクセスできるのでしょうか？
- 私たちのデータについて、SaaSサービスにどのように依存することになるのでしょうか？
- CSPの法的義務は何ですか？例えば、決済事業者は、マネーローンダリング対策（AML）を遵守するための法的義務によって、一部のデータを保持する必要があります。
- もし政府や軍関係者がデータへのアクセスを要求してきたら、SaaSプロバイダはどうしうるでしょうか？

例えば、機密データ（例：社会保障番号や財務勘定データ）ではなく、非機密データのみがSaaSアプリケーションに保存されている場合、サプライヤーの検証を減らした方が適切な場合があります。

管理策。

- 機密性の要件は、データの価値によって決まります
- データ分類の要件（例：HIPAA、PCI）
- データおよびメタデータの管理：所有権、処理、使用許諾
- データの所在と主権
- 可用性要件とデータモビリティ

3.1.1.7 プライバシー

SaaSプロバイダを利用する場合、利用者はそのプロバイダにデータを保存することによるプライバシーへの影響を確実に理解することが重要です。SaaS利用者は、SaaSアプリケーションに保存するデータについて、プロバイダに許容される利用方法があるかどうかを理解する必要があります（例：機械学習、匿名データセットの評価）。これらの用途は、もしあれば、SaaS利用者の規制および監査要件に直面します。

刻々と変化する規制環境は、それ自体がプライバシー関連のコンプライアンスまたはデータ所在地違反のリスクを高め、一部の利用者や特定の種類のデータに対するSaaSアプリケーションの配備を複雑にしています。欧州市民のデータを預かる米国SaaSプロバイダに関する他国からの懸念は、この潜在的なリスクを高めています。

管理策。

- SaaS利用者の役割とSaaSサービスの役割の対比
  - コントローラ（利用者またはスタッフのPII）
  - プロセッサ（コントローラから供給されるPII）
- プライバシーポリシー：SaaSプロバイダの自社サービス上のデータに対する権利
- 違反時の義務および責任
- PIIデータのインベントリ、可視性
- 同意の管理

3.1.1.8 詳細なリスクアセスメントを実施するためのステップ

1. 資産の特定
2. 脅威の特定
3. 脆弱性の特定
4. 測定基準の策定
5. 過去の侵害データの考慮
6. コストの計算
7. 流動的なリスクから資産への追跡の実施

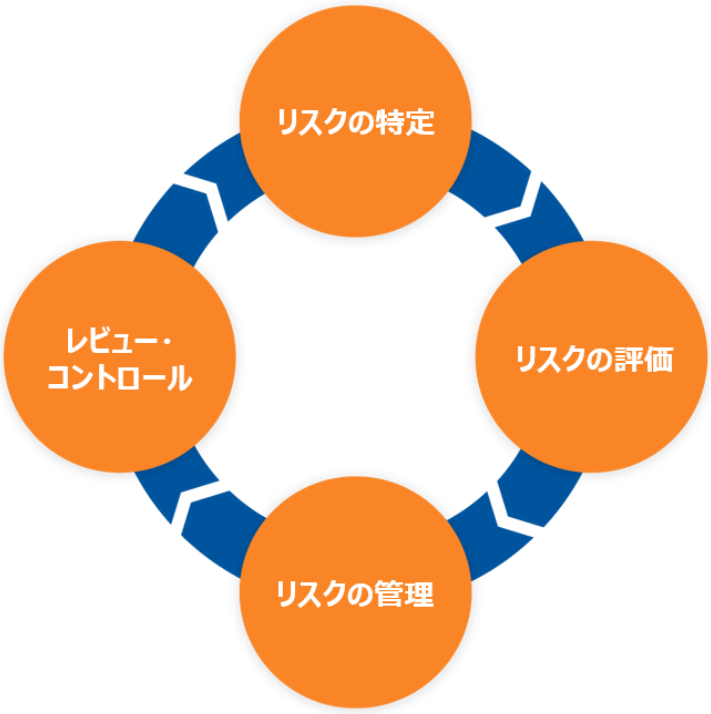

図2. リスクアセスメントサイクル

3.1.1.9 リスクの特定

ビジネス目標に支障をきたす可能性のあるリスク領域を特定します。

- データ、財務情報、知的財産/競争上の優位性の喪失
- 規制、法的義務
- 会社の評判
- 脅威、脆弱性、攻撃
- インシデント管理
- 技術的な複雑
  - 人材の専門性
  - 財務上のコミットメント
- サードパーティーサプライヤー
- 第三者監査、SOC2レポート、STAR Registryなど
- ヒューマンエラー

3.1.1.10 リスクの評価

- 定性的/定量的リスクアセスメント
- ガバナンス・リスク・コンプライアンス（GRC）
- リスク許容度/リスク選好

3.1.1.11 リスクの管理

- リスク許容度に応じた物理的、技術的、および/または管理的なコントロールの実装
- 第三者へのリスク移転
- リスクの受容

3.1.1.12 レビュー・コントロール

- 内部監査・外部監査
- リスク分析

リスクを特定するためには、SaaSサービスやCSPに関する詳細なリスクアセスメントが必要です。

企業資産をCSPのクラウドに預ける前に、リスクアセスメントを実施する必要があります。リスクアセスメントの詳細レベルは、環境によって異なります。例えば、限定されたユースケース（サンドボックス、ソフトウェア開発、CSPの機能やコントロールのテストなど）の下でCSPの使用を開始することを決定する場合があります。このシナリオでは、「最小限のリスク評価」が実施されることがあります。CSP のツールと機能が CSC のビジネス目標を満たす場合、アプリケーションが本番稼動に移行する前に、より詳細なリスクアセスメントを行う必要があります。

SaaSのリスクアセスメントを実施することを決定した場合、次の3つの領域を綿密に調査する必要があります：a）SaaSプロバイダ、b）SaaSプロバイダの管理手法、c）SaaSアプリケーションの技術的なセキュリティ上の考慮事項。以下の表は、考慮すべき点を列挙したものです。

プロバイダ	プラクティス	アプリケーション
CSPはどのような認定を受けていますか？	CSP はさまざまなリージョン/ゾーンとの間でデータを論理的に制限するために、どのような管理手段を採用していますか？	アプリケーション/特権アカウントは一元管理されていますか（例：IAM、RBAC、アカウント管理ツール経由）？
CSPは第三者による評価または監査を受けたことがありますか？CSPは、SOC II レポート（または同等のレポート）を提供できますか？	CSP はどのようなバックアップ／リストアサービスを提供しますか（例：アプリケーション、データ、VM）？	安全な経路が確保されていますか（例：パスワード、証明書、データの安全な転送）？
CSC のデータは CSP の施設内で保管されていますか、または CSP は（コロケーションのために：ping power pipe）サードパーティーサプライヤーとの間で契約を交わしていますか？	CSPのインシデント管理プロセスはどのようなものですか？インシデントはどのように分類されますか？	安全な認証のためにSSO/SAML/MFAが使用されていますか？

プロバイダ	プラクティス	アプリケーション
トラブルシューティングやメンテナンスなどのためにCSCに提供されるサポートはどの程度ですか？	VMイメージ、サーバー、データベースには定期的にパッチが適用されていますか？CSP のアンチウイルス管理プロセスはどのようなものですか？	アプリケーションやストレージのアカウントは公開されますか？
CSPのSLA/OLAはどのようなものですか？	暗号鍵どのように管理され、保管されていますか？誰がそれにアクセスできますか？	アプリケーション/ソフトウェアは、クラウド用にライセンスされていますか？
CSP はこの SaaS をサポートするすべてのサードパーティーサプライヤーのリストを提供していますか？その場合、CSP はバックグラウンドチェックと NDA を行なっていますか？	どのようなロギング/SIEMイベント脅威検知ツールが利用者に提供されていますか？	ソフトウェア/データは、規制やプライバシー要件の対象となりますか？
CSP はどの標準や規制要件に準拠できますか？ CSPはどの標準（例：ISO、NIST、CIS、PCI、HIPAA、GDPR）をベースラインコントロールにマッピングしていますか？	CSP はどのようなIDS/IPS ツールを提供していますか？	アプリケーションの開発/保守に必要なソフトウェア開発プロセス/ツールは何ですか（例：DevSecOps、GitHub、SDLC)？CSPはこれをサポートするために、どのようなツール/アプリケーションを使用していますか？
CSP の基盤となるアーキテクチャは、業界のベストプラクティスまたは標準を利用して設計/開発されていますか？	CSP は ハードニングされたVM イメージを提供しますか？どのように管理/実施されますか？	アプリケーションをサポートするためにどのようなAPIが必要ですか？CSP はどのようなサポートをしてくれますか？
CSP はクラウドリソースの自動化ツールやスクリプト（例：VM、IaC、自動修復）を利用/提供していますか？	CSP はデータの不正な流出を防止するための管理策を提供していますか？	CSP はアプリケーションの脆弱性/ペネトレーションテスト（必要な場合）をサポートしていますか？

誤解が生じないよう述べると、上記のリスク評価は、SaaSプロバイダのセキュリティと、使用されるSaaSアプリケーションの基盤となるアーキテクチャ及び実装に特化したものです。これはSaaS利用者によるSaaSアプリケーションの配備と使用に関する継続的なセキュリティ監視とリスクレビューを置き換えるものでは*ありません*。

SaaSのリスクを正しく管理するためには、様々なレンズを通してSaaSを理解し見ていく必要があります。そうして初めて、SaaSのリスクが適切に識別され、評価され、低減されたという一定程度の保証を得ることができます。リスクアセスメントは、「1回で終わり」と考えてはいけません。クラウドのリスクは流動的であり、定期的に、また重大な変更があるたびに実施する必要があります。

SaaS利用者は、自社のソリューションの要件を理解し、その要件がSaaSプロバイダによって理解され、満たされることを確認する必要があります。例えば、SaaSプロバイダが、あなたのアプリケーション/業界に必要な特定のサービス/コントロールを提供していないとします。そのような場合、SaaS利用者の責任において、そのギャップを低減するか、当該プロバイダを利用しないことを選択します。

3.1.1.13 クラウドプロバイダのベストプラクティスの検証

- サードパーティの技術サービスを組織の資産として扱います。
- サードパーティの評価に対するリスクベースのアプローチを確立します。
- 組織内の主要なステークホルダーからの情報に基づいて、サードパーティの評価を策定します。
- ビジネスオーナーの関与を確保します。
- リスクの高いベンダーを定期的に見直します。
- 認可されたベンダー/アプリの一覧を発行します。
- ビジネス上の正当な理由や承認がない限り、認可されたベンダー/アプリの使用を要求します。
- 組織全体で事前承認されたベンダーの使用を義務付けることを検討します。
- コンプライアンスを遵守するサプライヤーの使用を奨励または義務付けます。

3.1.1.14 ポリシー・プロシージャの策定

SaaSアプリケーションを安全に配備・利用するためには、SaaS利用者がSaaSアプリケーションの導入・利用状況を継続的に評価・監視するための社内ポリシーと手順を策定することが重要です。このセクションで前述した定期的なリスクレビューと評価は、SaaSプロバイダの技術、実務、認証を対象としていますが、SaaS利用者においても、SaaSアプリケーションの構成と実際の使用状況を対象とした監視と評価の方法論を整備することが、少なくとも同様に重要です。

このようなポリシーには、少なくとも、以下を含む必要があります。

- アカウント管理手順
- 一元化されたID管理手順
- データ及びシステムへのアクセス要件。すなわち、重要なアクセス権の付与の承認及び当該アカウントに対する追加的な認証の要求
- サービスの不正利用に対する利用規定
- ビジネスプロセスに対応した統合されたユーザーライフサイクル
- データの分類とラベル付け
- 既存のサービスレベル、インシデント、脆弱性管理プロセスへの統合
- 既存のガバナンスメカニズムへの統合、必要に応じた作成/更新、すなわち変更管理

他のセキュリティプログラムと同様に、SaaSアプリケーションの設定、データの分類及びデータアクセスの監視を、ある特定の時点の作業と見なすことはできません。SaaSは、他のクラウド技術よりもさらに変化が激しく、またすぐに再構成することが可能です。SaaS利用者の管理者は、不注意なコマンドやボタンのクリック一つでSaaSアプリケーションのセキュリティポスチャを大幅に変更することができることから、継続的な監視プログラムの必要性はさらに強調されることになります。

3.1.1.15 コンフィギュレーションとセキュリティポスチャ管理

重要なSaaSアプリケーションは、システムに保存されているデータの機密性や、漏洩した場合のビジネスの中断の可能性などの指標によって定義され、継続的に監視する必要があります。このような監視機能は、できれば自動化され、頻繁に実行され、大きな変更の後にアドホックに実行できることが望ましいです。理想的なのは、本番環境のSaaSで稼動させる前に、設定変更を検証するためサンドボックス環境や実稼働前の環境に対して実行してみる必要があります。

少なくとも、重要なSaaSアプリケーションに対するSaaS利用者のポスチャ管理プログラムは、次の点を考慮する必要があります。

- システム設定のうち、特に以下に関連する設定のためのコンフィギュレーションベースライン
  - アイデンティティ
  - MFA、SSO、地理的またはIPによる制限を含む、認証とシステムアクセス
  - パスワードポリシー
  - セッションコントロール
  - プラットフォームが提供するDLPと監査機能
  - プラットフォームが提供する暗号化機能、BYOK機能
- インストールされ承認されたサードパーティプラグインやインテグレーション、Oauth、もしくは他のクラウド間接続
- ロール、プロファイル、グループ、チーム、および追加のアクセスや機能を付与できるSaaSアプリケーション内のあらゆるエンティティへのユーザーの割り振り
- アクセス許可要素の設定とユーザーへの効果的なアクセス方法
- 機密または特権的な行動を示す可能性のある管理行動および権限ログ
- 主要なSaaSアプリケーションや環境におけるアクションの相関性
- 主要なタイプのデータまたはレコードへのユーザーアクセス、および読み取りアクセス（機密性）と書き込みアクセス（完全性）の判定
- オフボーディングの手順

この項のコンフィギュレーション管理とは、「構成管理」を指しています。 NIST 800-53のCM-2上では、*「ベースライン構成には、セキュリティおよびプライバシーの管理策の実装、運用手順、システムコンポーネントに関する情報、ネットワーク構成、およびシステムアーキテクチャ内のコンポーネントの論理的な配置などを含んでおり、システムの将来の構築、リリース、または変更の基礎として機能する。ベースライン構成を維持するには、組織のシステムが時間とともに変化するにつれて、新しいベースラインを作成する必要がある。システムのベースライン構成は、現在のエンタープライズアーキテクチャを反映している」*と述べられています。

クラウドのメリットのひとつは、ソフトウェア開発者が新しい機能、アプリケーション及びサービスを迅速に開発しやすくなることです。現今の主要なSaaSアプリケーションでは、重要なビジネスプロセスを制御するコードがほとんど無いもしくはノーコードのアプリケーションの作成とデプロイが含まれることがよくあります。これらのインテグレーション、ワークフロー、アプリケーションは、権限を持つユーザーによって迅速にデプロイ、変更することができます。そのため、このような権限がビジネスに与える潜在的な影響はさらに大きくなり、このような権限の不正な割り当てや使用に対して、監視や警告を行えることが重要となってきます。

さらに、SaaSアプリケーションの迅速な設定と、多くのSaaSプラットフォームにおけるクラウドアプリケーションマーケットプレイスの普及により、ユーザーは（SaaS利用者またはSaaSプロバイダのいずれによっても開発されていない）サードパーティ製アプリケーションでSaaSプラットフォームを迅速に拡張することができるようになります。これは強力な反面、ベンダーのリスク評価や調達プログラムからは見えない脆弱性をもたらす可能性があります。したがって、セキュリティ組織は、承認されたSaaSプラットフォームへのサードパーティ製アプリケーションの不正な接続を検出するための監視と警告の機能を備えていることが重要です。

1つのSaaSプラットフォームと他の1つまたは複数のSaaSプラットフォームを接続するSaaSエコシステムでは、統合前に権限と統合を正しく理解することが不可欠です。十分な統合情報が得られない場合、開発環境またはサンドボックス環境で統合を行う必要があるかもしれません。

例えば、マーケティングオートメーションプラットフォーム（MAP）とカスタマーリレーションシップマネジメント（CRM）プラットフォームを統合し、MAPのデータをCRMにフィードする必要がある場合を考えてみましょう。この場合、データがどこからどこまで流れるかを検討し、追跡する必要があります。MAPからCRMへ、あるいはCRMからMAPへ向けて流れるのでしょうか。この場合は、MAPからCRMへ向けたものとなります。

そして、CRMが事前に検証されたマーケットプレイスにおけるインテグレーションがあるかどうかを確認する必要があるでしょう。通常、マーケットプレイスからのインテグレーションは、ある程度安全です。

その後、ベストプラクティスのガイドラインを確認したり、ベストプラクティスが存在しない場合は、サポート担当者に連絡を取って入手することになるでしょう。

最後に、最小権限を確保し、データ最小化の原則に従う方法を分析する必要があるでしょう。

また、同様に接続を解除する方法も理解しておくことが不可欠です。

別の例として、ユーザーが自分のGoogleアカウントとサードパーティのアプリケーションを統合する場合を考えてみましょう。ユーザーは、サードパーティーアプリケーションがどのような権限とスコープを取得し、アプリケーションがユーザーの代わりにどのようなアクションを実行できるかを主に確認する必要があります。そして、組織のリスク選好度に基づいて判断してください。この点については、ユーザーはセキュリティの専門家のサポートを受ける必要があるでしょうし、サードパーティのアクセス権を取り消す方法も知っておく必要があるかもしれません。

セキュリティポスチャ管理ポリシーやルールを策定する場合、SaaS利用者は、業界全体のベストプラクティス（例：Microsoft 365のCIS Benchmark）を活用したり、調査を通じてセキュリティポリシーの基本方針を策定したSaaSセキュリティポスチャ管理ベンダーと協力したり、組織固有のベストプラクティスや要件を特定するための社内作業を実施したりすることが可能です。多くの場合、これらのオプションを組み合わせることで、最も包括的なポリシーが策定されることになります。

3.1.1.16 データセキュリティ

SaaS利用者は、システム構成やセキュリティのポスチャ監視と同様に、SaaSアプリケーションに保存された機密データへのアクセスを監視する必要があります。SaaSアプリケーション固有の柔軟性と設定可能性により、データに対するユーザーのアクセス権は迅速に変更される可能性があります。したがって、SaaSのセキュリティ監視の他の部分と同様に、データへのアクセスの監視を、ある時点の作業ではなく、継続的なプロセスとして扱うことが重要です。

データセキュリティとアクセス監視のソリューションの一環として、SaaS利用者は、データを機微レベルやデータの種類などによって、定期的に（または自動化されたプラットフォームの機能を使って）分類する作業を行う必要があります。この分類は、外部システムで管理されているか、SaaSプラットフォーム自体で管理されているかにかかわらず、データセキュリティポリシーを設計し、それに照らして実際の状態を監視する上で極めて重要となります　。

データセキュリティに関するその他の考慮事項として、セキュリティポスチャ監視の一環として監視できる可能性が高くても明確に定義しておく必要があるものは以下のとおりです。

- データエクスポート機能およびデータバックアップ機能の設定（およびユーザーアクセス）
- 資産、所有権、責任のインベントリ
- 社内外の共有の制限とそのポリシーに合わせたシステム構成の監視
- 暗号の制御と要件、およびシステムが意図したとおりに構成されていることを確認するための監視

SaaSアプリケーションに適用可能なセキュリティソリューションのもう一つの種類は、データ損失防止（DLP）ソリューションです。DLPソリューションは、多くの場合、データへのアクセス経路にインラインで配置されたり、SaaSアプリケーションの組み込み機能として提供されます。データ損失防止は、より高度な情報保護を実現するために役立ちます。特定の種類の文書の転送や流出を防止することができます。DLPソリューションは、データ分類にも関係しています。まず、DLPソリューションが分類を理解し、それに応じて監視できるデータやドキュメントを分類する必要があります（例：PII、PCI）。

DLPは主にキーワード、フレーズ、及びメタデータに基づいて動作します。DLPロジックと一致した場合、ユーザーへの通知、管理者への警告、送信のブロック、添付ファイルや文書の削除、機微データのマスキング、検査/フォレンジック目的のためにデータのコピーを保持するなど、1つまたは複数のアクションを実行することができます。SaaSプロバイダは通常、このプロセスを自動化するための仕組みやAPIを利用者に提供します。多くのSaaSシステムを利用している場合、SaaSプラットフォームと統合してシームレスに管理できるDLPソリューションが好まれます。

3.1.1.17 ユーザーへの啓発とトレーニング

- 本サービスを安全に利用するためのベストプラクティスガイドラインの策定
- データの分類とラベル付けの実施
- 本サービスにおけるセキュリティインシデントが何かとその報告方法に関するユーザー啓発
- 可能な限りのコーチングポリシーの追加（例：ユーザーは、カテゴリに対して認可されたサービスにアクセスするよう促されるか、代替サービスの使用について正当な理由を記録するよう求められます）
- 忌憚のない報告をするための雰囲気作りの醸成

3.1.1.18 内部脅威

- 退職した従業員が個人アカウントとSaaSのデータを共有する可能性がある。これにより、企業データが流出する可能性があります
- 従業員が機密データを社内で過剰に公開する（財務部門とエンジニアリング部門が互いの情報を利用する可能性があります）
- 機密性の高いデータを誤った第三者と共有しています
- 職務が分離されていない
- データ流出の原因となる不適切なプラットフォーム設定（機密データを含むS3バケットが公開されるなど）
- 従業員に、システムのデータダンプ取得が許可されていることにより、退職時にデータが漏洩したり、持ち出しされる可能性があります

3.1.1.19 外部脅威

- サードパーティの協力者が、企業データに永久にアクセスすることができます
- ベンダーが、企業データをサードパーティのリスクアセスメントを経ていない他ベンダーと共有しています
- ほとんどの場合、多要素認証が設定されていない個人アカウントで企業データを扱うサードパーティの協力者
- サードパーティベンダーまたはその下請け業者やサプライヤーが、データ保護について規制当局に拘束されません

3.1.2 使用方法

- 許容範囲内の使用
- 管理
- ガバナンス

3.1.2.1 サービス／サプライヤーの定期的なレビュー

- サービス利用規約の変更の監視及び各版のアーカイブ
- セキュリティ保証の有効性
- 継続的なセキュリティパフォーマンス

CSPサプライヤーの管理は難易度が高いです。

3.1.2.2 アラート

- 不審なログインやデータアクセスの監視
- サービスの利用状況や不正利用の監視
- SLA遵守のためのサービス属性の監視
- ログインやアクセスに関する異常の監視
- リスクとなる組織全体の設定変更の監視
- データへの異常なアクセスの監視

サービス利用規約が一夜にして変更され、制御不能になることがあります。そのため、自動化されたツールを使って、サービスの属性を継続的に監視します。

設定変更を監視し、必要に応じて警告を発します。

3.1.2.3 使用状況の可視性

- ログイン、ユーザーロケーションを含む認証ログ
- アクセスログ
- 監査ログ
- アカウントのプロビジョニングとデプロビジョニングのログ

3.1.2.4 継続的な評価と攻撃対象領域の低減

- サービスの基本属性を監視し、健全性を確認する
- 攻撃ベクトルを減らすためのコントロールの見直し
- 内部故障の可能性のある箇所を監視する

3.1.2.5 コンフィギュレーション管理

- 設定変更を監視し、必要に応じて警告を発する

3.1.2.6 データ

- 機密データ、システム、フィールドへのアクセスの監視
- 行政処分の監視
- 監査を有効にする
- 有効なバックアップの監視

データのバックアップを確実に実行します。そしてさらに重要なことは、リストアを実行またはリクエストすることによって、バックアップをテストすることです。

3.1.3 契約解除

SaaSの利用を終了するには、調整と計画的な実行が必要です。

SaaSサービスのリスクとして最も重要でありながら見落としがちなのが、CSPが提供する契約です。

組織は従来、法務部門と協力し、サービスプロバイダの契約条件を「ベンダーフレンドリ」ではないように交渉し、サービスプロバイダによる損失を、プロバイダに金銭的な責任を負わせることで軽減してきました。しかし、クラウドプロバイダは、通常の補償、責任制限、その他の条件、特にプライバシーとデータセキュリティに関する条件を提示することに積極的ではありません。

CSPが最もよく挙げる理由は、これらの追加的な義務や責務が、クラウドコンピューティングの低価格モデルを脅かすこと、そしてCSPは利用者がクラウド上に何を保存しているかを知らないため、利用者データの分離と安全確保について責任を負うことができないことです。ただし、CSPは、利用者がこれを達成するための手段を提供する必要があります。

クラウド契約における不利な条件は、クラウドサービス利用者のリスクを増大させる可能性があります。

また、クラウドサービスの利用者は、利用者のデータを保存または処理するためにCSPが利用する下請業者を契約上制限することもできます。このような制限が無い場合、利用者は自分のデータが実際にはプライマリCSPから2～3ホップ離れていることを知るかもしれません。

3.1.3.1 内部プロセス

- サービス終了を全ユーザーに通知
- すべてのAPIアクセスを無効にします
- 置換またはデータ抽出に関するガイドライン
- 将来の利用や新サービスへの移行のためのデータ抽出
- どこに保管し、誰が責任を負いますか？
- 他のシステムとの統合やデータフローをすべて理解していること

3.1.3.2 データ保持

- バックアップや残存データ・メタデータの破棄（システムログ、監査ログ、アクセスログ、検索インデックスなど）
- データ保持期限は、データ分類の要件を満たす必要あり
- 財務情報のエクスポートと削除
- 使用状況などのレポートのエクスポート

3.1.3.3 資産の返却

- データ/メタデータのエクスポート（監査ログ、アクセスログ、バックアップなど）
- データロケーションの要件に準拠します
- 使用可能なデータフォーマット
- 納期、納品方法、いつまで利用可能か

3.1.3.4 サービス専用アタッチメントの廃止

- サービス別モニタリング
- サービスのセキュリティ監視

3.1.3.5 サービスマネジメント

- サービスとの統合をすべて解除
- サービスの廃止を確実にする
- 契約の確実な締結

3.2 情報セキュリティに関するポリシーの見直し

テクノロジーは頻繁に変化するため、ポリシーを見直す定期的なサイクルが必要です。前回のバージョン以降、追加の許容範囲内のコントロールが必要になる場合があります。また、SaaSの運用は、組織が定めた必要最低限の基準を満たしている必要があります。

CASBのような一部のソリューションプロバイダは、SaaSサービスの継続的な評価とスコアリングを行い、これらの動的なスコアに基づいてアラートとアクセスポリシーを設定する機能を提供します。

4. 情報セキュリティ組織

4.1 内部組織

4.1.1 情報セキュリティの役割と責任

多くの人がSaaSをアウトソーシングと捉えていますが、クラウドサービスカスタマ（CSC）とクラウドサービスプロバイダ（CSP）間の役割と責任（R&R）を明確に理解することは不可欠です。CSCがCSPと契約する前に、デューケアとデューデリジェンスを行えば、思い込みや誤解を緩和することができます。また、CSPとCSCの責任を明確にすることにも役立ちます。CSPがどのような責任を負うかよりも、何に責任を持たないかを知ることが重要であるとも言えます。

「R&R」がCSPとCSCの間でどのように分担されているか（責任共有モデルに記載されている通り）をよく理解すれば、CSCがコントロールできない部分が多くあることが明らかになるでしょう。一般に、ほとんどのSaaSの実装において、アプリケーションやデータへのアクセス権の付与は、CSCに責任があるとされています。同時に、CSPはそれ以外のすべてに責任を負います（たとえば、SaaS利用者は、自分の管理下にない既知のVMの脆弱性を軽減することはできません）。これにより、CSCはセキュリティとメンテナンスの大部分をCSPに委ねることになります。

CSCが責任を負うべきSaaSソリューションの機能があります。CSCはこの課題を受け入れ、時間をかけてリスクを理解し、それに見合ったレベルまでリスクを低減させなければなりません。
SaaS アプリケーションが、弱い TLS 暗号(例えば、TLS 1.2)を受け入れる場合を考えてみましょう。利用者は、古いバージョンの使用を禁止し、アプリケーションにTLS 1.3のみを受け入れるように強制することができます。別の例として、ユーザー認証にActive Directoryの利用を義務付けるなどもあります。

とはいえ、SaaSの利用者は、SaaSプラットフォームへの依存から生じるセキュリティリスクや運用リスクから資産やリソースを保護するために、管理的コントロールと技術的コントロールの両方を組み合わせる必要があります。以下の表は、CSCが実施すべきコントロールを示したものです。実際の技術的コントロールは、CSPによって異なることに留意してください。

技術的コントロール	管理的コントロール
セキュリティ監査/ロギング用のシステムやアプリケーションアカウン	ユーザー/システム認証
特権アカウントの多要素認証(MFA)	ユーザー/システム認証
特権アカウントのシステム監視	毎年のアカウント所有者によるすべての特権アカウントの必要性の監査証明

技術的コントロール	管理的コントロール
全アカウントのIAM（Identity and Access Management）ツール	暗号鍵の所有者の識別
暗号鍵、電子証明書などの安全な保管場所	すべてのCCのリソース/資産のインベントリ追跡
安全な通信経路（例：HTTPS、SSH、TLS、SFTP）	ネットワーク/アーキテクチャーチームからの承認
すべてのクラウドリソース/資産に対する単一の「ガラス窓」（例：SIEM、ログ統合）	• ユーザー認証 • 指標 • コンプライアンスの報告
脆弱性管理 パッチ管理 是正・修正	脆弱性の分類 脆弱性の通知
インシデント管理ツール	インシデントの特定、伝達、管理方法に関するCSP/CSC間の連携
リスクマネジメント評価ツール（以下を含むことができる）： • 脆弱性スキャン • 脅威モデル • ペネトレーションテスト	• リスクマネジメントの承認・見直し • 主なリスク指標 • 関連するステークホルダーへの調査結果の伝達 • 知識移転

注：CSCとCSPの共有責任の詳細についてはCSAのエンタープライズアーキテクチャ - CCM責任共有モデルを参照してください。

4.1.2 職務の分離

セキュリティ原則である職務の分離（SoD）を実施するためのコントロールが必要です。職務の分離とは、簡単に言えば、重要な業務を遂行するために2人以上の人物・組織を必要とすることを保証し、不正・癒着を防止することを目的としています。

NIST 800-145の「クラウドコンピューティング」の定義を参照すると、クラウドの特徴として「オンデマンドセルフサービス」が不可欠とされています。「オンデマンドセルフサービス 」とは、「利用者が一方的にサーバーの稼働時間やネットワークストレージなどのコンピューティング能力を、人の手を借りずに自動的に必要に応じて調達できる」ことを意味します。 つまり、「オンデマンドセルフサービス」というクラウドの特性により、クラウドコンピューティングはエンドユーザーに技術的な専門知識をあまり要求せずに、非常に迅速かつ容易にクラウドのリソースと資産を追加することができます。これは、SoDの施行が非常に複雑になり、制御不能になりやすいということでもあります。

ユーザーやアプリケーションが作成／スピンアップするクラウドリソースは、さまざまな形態（ユーザー／システム／アプリケーションのアカウントID、ロール、グループなど）で提供されます。利用者は、これらのリソースがアクセスできる対象（クラウド境界の内外）、それらのIDに関連する権限を理解し、それらのアカウントが特定のタスクを実行するための最小限の権限を持つように、適切な措置を講じる必要があります。これを怠ると、アカウントがリソースに意図しないアクセスを持つ可能性につながります。SoDコントロールを行わない場合のリスクとしては、機密情報・プライバシー情報の不正な漏洩、データの損失、完全性の喪失などがあります。

4.1.3 当局との連絡

CSPがクラウドソリューションの維持に関連するタスクの大半を所有していても、CSCはクラウド内で発生するすべてのことに責任を負います。これは、CSCが契約を締結する際に、CSPが提供する「利用規約」、「提供サービス」、「制限事項」に同意しているためです。

CSCは、インシデント発生時やSLA/OLA（Service Level Agreement/Operating Level Agreement）の変更時に通知される主要関係者を特定するプロセスを文書化しておく必要があります。CSCはこれをCSPと共有し、CSP は（インシデント発生時に）誰に連絡すればよいかを知ることができます。これらのステークホルダーは、ビジネス目標/成果物やコンプライアンス/規制要件を強く意識すべきです。

4.1.4 専門研究グループとのコンタクト

クラウドセキュリティに対するリスクは日々変化しており、把握することはほとんど不可能です。組織は、特別な専門研究グループとの接触を確立・維持することを任務とする特定の担当者／チームを特定することを強く推奨します。これらの専門研究グループは、新しい脆弱性や「ゼロデイ」脆弱性を追跡し、また、これらの脆弱性の一部に対する可能な修正策を共有することもあります。専門研究グループと関係を持つことは、企業の時間を節約することになります（修正点を発見する時に）。もう一つの利点は、企業が自社のニーズに最も関連する特定の研究グループを選べることです（例：産業、技術、規制）。最後に、これらの専門研究グループは、新たなトレンド、プライバシー、脅威、脆弱性、改善策に関連する最新情報を提供することもできます。

4.2 モバイル端末とテレワーク

4.2.1 モバイル端末ポリシー

COVID-19は、誰も予想できなかったほどのインパクトを与えました。多くの企業が、事業を継続するために在宅勤務のソリューションを提供することに躍起にならざるを得ませんでした。

SaaSサービスでは、モバイル端末向けのWebフロントエンドや、モバイル端末にインストールするSaaSサービス専用のアプリケーションを通じて、モバイル端末からのアクセスを提供します。そのような端末は、個人/会社支給のノートパソコン、個人/会社支給の携帯電話、またはタブレット端末の形があり得ます。COVID以前の状態に戻るかどうかは、誰にもわかりません。そのため、安全な継続的運用を促進するためのポリシー、手順、ガイドラインを作成する必要があります。

CSC は、モバイル端末による企業リソースへのアクセスを許可することに関連するリスクを特定しなければなりません。以下は、検討すべき分野の一例です。

- 誰が会社のリソースにアクセスできるのですか？
- アクセスできるのは社員だけですか、それとも契約社員や第三者であるサプライヤーもアクセスできますか？
- 誰もがアクセスできる会社のリソースとは？
- 契約社員や第三者であるサプライヤーに対して制限すべき会社のリソースとは？
- VPN、ソフトトークン、MFAなど、どのようにアクセスを許可しますか？
- 個人所有のデバイスで会社のリソースにアクセスすることを許可すべきでしょうか？
- 個人所有のデバイスを許可した場合、マルウェア、フィッシング、なりすまし攻撃などから企業のリソースをどのように保護すればよいのでしょうか？
- 社員や契約社員にアクセス権を与えた後、彼らが明示的に権限を与えられたリソースにしかアクセスできないようにするには、どうすればよいでしょうか？
- アクセスはどのように監視/記録されるべきですか？
- 会社の機密情報が盗まれたり、社外（あるいは権限のない人や競合他社に）に移されたりしないようにするには、どうしたらよいでしょうか？
- 社員が退職する場合、会社のデータがその社員と一緒に持ち出されないようにするためには、どのような対策が必要でしょうか？

CSCが考慮しなければならない技術的コントロールとは別に、以下のような管理的コントロールも考慮しなければなりません（すべてを網羅しているわけではありません）。

- セキュリティ意識向上トレーニング
- 利用規定
- データ分類の基準/方針
- 機密・秘密情報の取り扱い
- メディアの取り扱い
- リムーバブルメディアの使用
- 暗号化（会社支給の端末の場合）
- 物理的コントロール（会社支給の端末の場合）
- データの保持・破棄

5. 資産管理

SaaSサービスの恩恵を受けるために、SaaSの利用者はSaaSサービス上で処理される特定のデータを提供する必要があります。そのため、SaaSの利用者にとって、データの管理は非常に重要です。

5.1 資産に対する責任

5.1.1 資産のインベントリ

SaaSの利用者は、以下の質問に答えることができるはずです。

- SaaSサービスにはどのようなデータが転送されるのでしょうか？
- データはどのように転送されるのですか？
- SaaSサービスはどのようなデータにアクセスできますか？
- 我々のデータのSaaSサービスへの依存度は？
- 規制や顧客サービスの要件など、データに対する地理的な要件がありますか？
- 組織全体でどれだけのSaaSアプリケーションを利用していますか、シャドーSaaSは存在しますか？
- CSCは、もはや使用されていないリソースを特定することができますか？未使用の（しかし有効になっている）リソースがあると、運用コストがすぐにかさんでしまいます。
- CSCは、すべてのクラウドホスティング化されたリソースを容易に特定できますか？CSCは、資産の所有権と責任を文書化した企業内集中管理レポジトリを持つべきです。また、CSCは全社的なタグ付けの方針とスキーマを策定する必要があります。タグ付けは、CSCが地理的な位置、機密性、法的義務、コストの最適化、その他多くの属性によってクラウドリソースを分類することを可能とすることから、タグ付けは、CSCにクラウドホスティング化されたリソースの正確な追跡を容易にし、企業のセキュリティガバナンスの活動を支援することができます。

5.1.2 資産のディスカバリ

組織内のユーザーによるSaaSの利用を継続的にディスカバリし、特定するためのプロセス、理想的にはソリューションが必要です。それは、以下の4つの異なる方法のどれかで実現できます。

- SaaSの購入や取得の可能性がある場合、利用前にITとセキュリティの部門に持ち込む手続き方法によります
- ファイアウォール、Webゲートウェイ、CASBからのログの解析・評価を通じて
- SaaS Security Posture Management（SSPM）ソリューションの活用により
- 経費報告書や財務記録からSaaSに関連する項目を分析することにより

5.1.3 資産の所有権

SaaS利用者は、以下の質問に答えることができるはずです。

- SaaSサービス上にどのようなデータが置かれているか、誰が責任を負いますか？
- SaaSの管理者は誰ですか？

5.1.4 許容できる資産の利用について

これには2つの部分があります。

- SaaSプロバイダは、利用者のデータ、メタデータに対して何をすることが許されているのでしょうか？
- SaaSサービス上のデータについて、当社のユーザーは何をすることができるのでしょうか？

データおよびメタデータのコントロール：所有権、処理、ライセンス。

6. アクセス制御

6.1 アクセス制御のビジネス要件

6.1.1 アクセス制御ポリシー

- リソースへのアクセスを必要としているかどうかを評価します
- ビジネス要件と役割の明確化
- データ分類に基づく情報クリアランス
- セキュリティレビューとデータオーナー（スポンサー）による承認

組織内のユーザーは、通常、過去のイベントに基づいて、または同僚のアクセス権を複製することによって、アプリケーションへのアクセス権を付与されます。

そのため、その人が本当にサービスにアクセスする必要があるのかを評価し、ビジネス上の要件を確認し、役割を設定することが重要です。

6.2 ユーザーアクセス管理

クラウドのリソースを保護するためには、アイデンティティとアクセス管理（IAM）を適切に管理・設計することが不可欠です。プラットフォームを導入する際には、セキュリティとビジネス要件を考慮し、職務やビジネス要件に応じた適切なユーザーグループ分け、分離、必要な権限の割り当てを行うことが不可欠です。適切なIAMの実践は、最小限の特権と職務の分離を強制します。

6.2.1 ユーザー登録・解除

6.2.1.1 ユーザーアクセスプロビジョニング

- ベストプラクティスに関するユーザートレーニング
- 使用許諾、関連するポリシー、手順に関する認識
- ユーザーアクセスベースラインに応じたアカウント作成
- 入社、異動、退社のプロセス全体の一部である必要があります
- 可能な限りロールベースアクセスを活用し、最小権限を遵守します
- 請求先：使用量に応じたグループまたはスポンサー？
- リソース制限の確認と設定

常に最小特権の概念に従い、リソースの制限を確認し設定します。

6.2.2 特権的なアクセス権の管理

- 特権的なアクセスが必要であることを確認するために、正当な理由を求める必要があります。
- 必要なときだけ権限を昇格させ、非特権アクセスに戻すジャストインタイムアクセスの使用を検討します。
- 特権的なアクセスを必要とするユーザーの数は最小限にとどめるべきです。

6.2.3 秘密認証情報の管理

- Break glass アクセス（緊急アクセス用管理者アカウント）は、非常に特殊な目的のみに使用し、認証情報は適切なセキュリティレベル（例：Key Vault）で保管する必要があります。

6.2.4 ユーザーアクセス権の見直し

- アクセス権は、ビジネスの変化に合わせて、適切であることを確認するために、定期的に見直す必要があります。

6.2.5 アクセス権の削除または調整

- アカウントの即時停止を確実にします
- アカウントに関連した停止したリソース課金
- 監査ログやアクセスログは、ビジネスポリシーに沿って保管されねばなりません
- 必要に応じてセキュリティの見直し
- アカウント終了ログとインベントリの更新

セキュリティポリシーに基づき、監査ログがレビューされ、保持されていることを確認します。

そして最後に、リソースが使用されなくなったときに課金を停止するようにします。これを自動で行い、手動での操作を一切排除するようにします。

6.2.6 ユーザーアクセスの監視

- 基本的な使用プロファイルに基づいた監視アラートの設定
- 不審なログイン（場所、時間など）、データアクセス（バッチアクセスなど）に対するアラート機能
- パスワードポリシーの遵守
- データ損失防止監視
- アラートを設定し、不審な行動やログインを監視することで、社外／契約社員の行動と社内社員の行動を区別します。
- APIベースのソリューションを活用した静止データの監視

6.3 システムおよびアプリケーションのアクセス制御

6.3.1 情報アクセス制限

- SaaSアプリケーションに保存された情報は、SaaS利用者のビジネスセキュリティポリシーに準拠した承認されたデバイスから認証されたユーザーのみがアクセスできるようにする必要があります。アプリケーションの性質上、これが実行不可能な場合（例：外部とのコラボレーションアプリケーション）、リバースプロキシなどの他のソリューションが、必要なきめ細かいアクセス制御を提供する上で役に立つかもしれません。

- APIベースのソリューションは、保存中のデータの保護、適切な共有とDLPポリシーの適用に活用できます（例：PIIを含む文書を外部ドメインと共有すると、自動的に内部ユーザーのみへのアクセスに戻ります）。SaaSアプリケーションは公共のインターネット上で利用できるため、可能であれば、アクセス範囲を承認されたIP範囲/場所のみに制限する必要があります。
- SaaSアプリケーションに格納された情報をダウンロードする必要がある場合（アクセス後）、適切なセキュリティ管理が導入され、情報がビジネスのセキュリティポリシーに準拠した承認済みのデバイスにダウンロードされることを確実にする必要があります。
- SaaSアプリケーションの認可されたインスタンスと認可されていないインスタンスを区別し、それに応じて使用ポリシーを適用できることが重要です。
- APIを使った第三者へのアクセスは、適切なチェックを経てから承認し、ビジネス要件が満たされた時点で取り消す必要があります。
- SaaSプロバイダがSaaS利用者のデータにアクセスする必要がある場合、プロバイダに通知し、要求を評価し、要求を承認/拒否する能力を持つ必要があります。

6.3.2 セキュアなログオン手順

- Basic認証を有効にしてはいけません。これは本質的にセキュアではありません。
- 可能であれば、SaaSアプリケーションは、ビジネスのアイデンティティプロバイダー（IdP）を使用し、シングルサインオン（SSO）によりセキュアにログオンできるようにする必要があります。
- SSOが不可能な場合、SaaSアプリケーションは、複雑かつ非公開のパスワードを強制する必要があります（たとえば、https://haveibeenpwned.com/ で検証します）。このパスワードは、会社のパスワードと同じであってはなりません。
- SaaSアプリケーションは公共のインターネット上で利用可能であるため、ユーザーが本人であることを保証するために、多要素認証を導入する必要があります。
- ユーザーは、ビジネスセキュリティポリシーに準拠した承認済みのデバイスからのみ、SaaSアプリケーションにログオンする必要があります。
- セキュアログオンに失敗した場合、パスワードのリセット方法はセルフサービスであるべきです。

6.3.3 パスワード管理システム

- 可能であれば、SaaSアプリケーションはパスワードを管理する必要がなく、代わりにビジネスのIdPを利用してSSOでユーザーを認証する必要があります。
- ローカル認証を使用する場合、パスワードはOWASPが定めたガイドラインに従うべきです。

また、パスワードは、機密性、完全性、可用性を保護するために、Key Vaultまたは同様のセキュリティデバイスに保管する必要があります。

パスワードは「クレデンシャル」であることに留意してください。この議論のために、「クレデンシャル」は暗号鍵、デジタル証明書、および／またはトークンの形 で提供されます。CSCが鍵を管理できない場合、鍵の保管庫または同様のセキュリティソリューションを利用し、機密性、完全性、可用性を強制することが強く推奨されます。

6.3.4 特権的なユーティリティプログラム/サードパーティプラグインの使用について

- Basic認証をプログラムで行うことは禁じられます。
- 呼び出し元のIDは、mTLSによって検証しなければなりません。
- トークンベース認証（OAuth 2.0）フローが望ましい。
- SaaS APIは、特定のIPの範囲内でのみ利用可能でなければなりません。
- Secure Vaultを構築し、特権的な資格情報を暗号化して保管します。
- APIのキーは安全に保管されなければならず、HTTPS上でのみ送信されなければなりません。
- SaaSアプリケーションは、アクセスキーとトークン付与を無効にする機能を有しなければなりません。
- 特権的なプログラムアクセスに使用されるIDは、定期的に見直されなければなりません。
- サードパーティアプリに対するユーザーからの同意を確認します。
- サードパーティアプリによるアクティビティを監視します。

6.3.5 プログラムソースコードへのアクセス制御

- ソースコードへのアクセスはSaaSプロバイダに限定されなければなりません。
- ソースコードを生成する開発パイプライン/環境に対するアクセス制御も、SaaSプロバイダに限定されなければなりません。
- ソースコードは、SaaSプロバイダの管理下にない他のプログラムやシステムへのバックドア・アクセスや、SaaS利用者へのセットアップの一部を提供してはなりません。
- SaaS利用者が作成したソースコードは、作成したバックアップとともに、利用者のみがアクセス可能でなければなりません。CSCは、CI/CDパイプラインを使用する場合、どのようなセキュリティゲートを実装するか、また、どのイベントがセキュリティレビューを引き起こすかを記述したプロセスを文書化しなければなりません。セキュリティゲートとは、ソフトウェアのセキュリティリスクを評価するセキュリティポリシーのことです。次のフェーズに移行する前に、すべてのソフトウェアコードがレビューされ、承認されなければなりません。

7. 暗号化および鍵管理

7.1 SaaS環境におけるデータセキュリティ

SaaSサービスを利用する際に最も重要な側面の一つは、そのサービス内に保存されるデータのセキュリティです。この運用モデルでは、ベンダーがアプリケーションのセキュリティに対する責任の多くを負うことになります。しかし、責任共有モデルでわかるように、データはクラウド利用者の責任です。

SaaSプロバイダへのデータ転送や保存に係る安全性を確実なものにするために、データの暗号化とそれに使われる暗号鍵の管理は、利用者がこれらのベンダーと契約するにあたり考慮すべき事項の一つです。データを社内の安全な場所から移動させる場合、そのデータを偶発的または悪意により外部へ流出させるというリスクが利用者組織にあります。適切な暗号化と鍵の管理を確実にすることは、万が一不正なアクセスが発生しても、まずデータを復号しなければ利用不可能であることを意味します。

このセクションでは、SaaSプロバイダに保存されたデータが、管理の行き届いた暗号鍵を使用して適切に暗号化されていることを確実にするために、利用者組織が取ることのできる手順を概説します。

7.1.1 責任共有モデル

SaaSサービスを利用するにあたり、アプリケーションの管理・保守の責任の一部は利用者組織からベンダーに移行しますが、一部の責任は利用者に残ります。これらの責任は、SaaSサービスにおけるデータのガバナンスとセキュリティ、およびサービスに使われるアクセスモデルを含みます。

	責任	SaaS	PaaS	IaaS	オンプレ
責任は常に利用者が保持する	情報・データ	●	●	●	●
	デバイス（モバイル、PC）	●	●	●	●
	アカウント、ID	●	●	●	●
責任はタイプにより変化する	アイデンティティとディレクトリのインフラストラクチャ	●●	●●	●	●
	アプリケーション	●	●●	●	●
	ネットワーク制御	●	●●	●	●
	オペレーティングシステム	●	●	●	●
責任はクラウドプロバイダへ移行する	物理ホスト	●	●	●	●
	物理ネットワーク	●	●	●	●
	物理データセンター	●	●	●	●

● マイクロソフトの責任　● 利用者の責任　●● 責任の共有

7.2 SaaSプロバイダと共有するデータの暗号化

前述したように、データが社内の安全な場所から移動するときはいつでも、偶発的または悪意による外部への流出のリスクがあります。このリスクを軽減する最善の方法は、SaaSプロバイダとの間のデータ転送と、SaaSプロバイダのシステムに保存されるデータの暗号化を確実にすることです。これは、SaaSプロバイダの責任であるアプリケーションと物理リソース内の適切な暗号化の確保を含みます。

7.2.1 疑問点・検討すべき点

必要な暗号化のレベルと暗号化が必要な場所は、転送されるデータとSaaSプロバイダの実務の理解に依存します。下記は、データ保護に必要なレベルを決定する際に考慮すべき論点です。

7.2.1.1 SaaSプロバイダへの質問

- ベンダーは、データ共有のためのきめ細かいコントロールを提供していますか（例：社内のみでの共有、選択したパートナーとの共有、関係者全員との共有など）？
- SaaSプロバイダは、転送中のデータの暗号化を提供していますか？
- SaaSプロバイダは、保存データの暗号化を提供していますか？
- SaaSプロバイダは、エンドツーエンドの暗号化をサポートしていますか？
- SaaSプロバイダは、どのような暗号化アルゴリズムと転送プロトコルをサポートしていますか？
- SaaSプロバイダは、利用者ごとに個別の暗号鍵を提供していますか（シングルテナント）？
- SaaSプロバイダは、鍵の管理手順に関する文書を提供していますか？
- SaaSプロバイダは、利用者が管理する暗号鍵の使用を許可していますか？
- SaaSプロバイダは、墨塗りデータを特定および/またはマスキングする機能を有していますか？
- SaaSプロバイダは、本番データをサンドボックス環境に複製する必要がある場合、仮名化を許可したり、秘匿すべき情報を除去したりしてしていますか？
- SaaSプロバイダは、ユーザーが機密データやフィールドにタグ付けする仕組みを提供していますか？

7.2.1.2 社内での質問

- SaaSプロバイダにアップロードされるデータには、機微情報が含まれていませんか？
  - 機微なデータには、個人を特定できる情報（PII）や、データプライバシーやコンプライアンスのニーズによって定義されたその他の要素のようなものが含まれることがあります。
- 万が一データが外部へ流出した場合、利用者組織にはどのような影響がありますか？
- あなたは、あなたの組織の鍵管理に自信がありますか？
- 内部プロセスは、エンドツーエンドの暗号化をサポートしていますか？

7.2.2 転送中の暗号化

データは、ある場所から別の場所に移動するときに「転送中」と考えられ、これは利用者組織からSaaSプロバイダに、またはその逆に移動するデータを含みます。データのセキュリティは、相互運用可能な複数のレイヤーが構成されているときに最も強固になります。したがって、データ転送中に、データ保護に利用可能なレイヤーが少しでもあると、データのセキュリティはその分だけ低くなると考えられています。

転送中のデータを保護するために、すべてのデータ転送においてセキュアな暗号化ネットワークプロトコルの使用を確実にすることが推奨されます。書き込みの際、使用するべき暗号ネットワークプロトコルのうち最良のものは、TLS（Transport Layer Security）バージョン1.2以上（TLS 1.3が望ましい）です。高いレベルでは、TLSプロトコルは共有鍵暗号（データの暗号化と復号化に同一の鍵を使用する方式）と公開鍵暗号（数学的に関連した公開鍵と秘密鍵を、データの暗号化と復号に使用する方式）の組み合わせを使用します。このような暗号化方式の組み合わせ手法は、転送中のデータの機密性と完全性を強化します。

TLS 1.3の使用は、セキュリティ面を犠牲にすることなく、パフォーマンスのためにTLS 1.2からいくつかのステップを削除しています。TLS 1.2と1.3のためのTLSハンドシェイクおよび鍵交換プロセスは、下の例のように動作します。

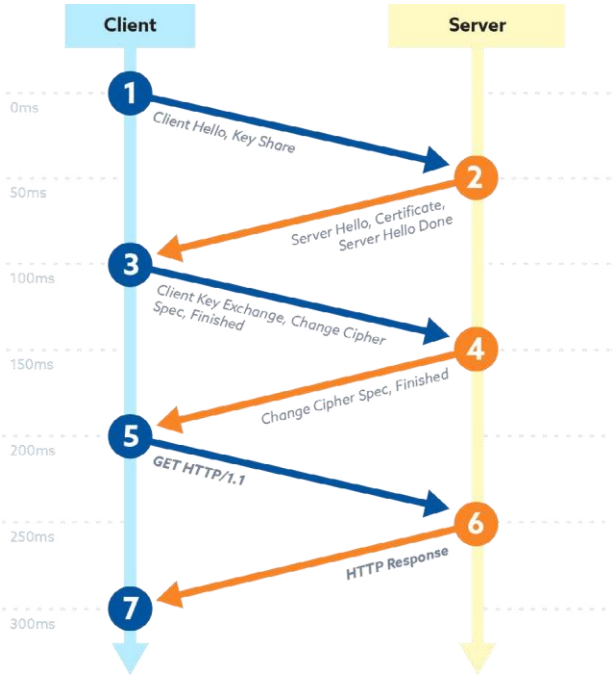

図3.TLS 1.2（フルハンドシェイク）

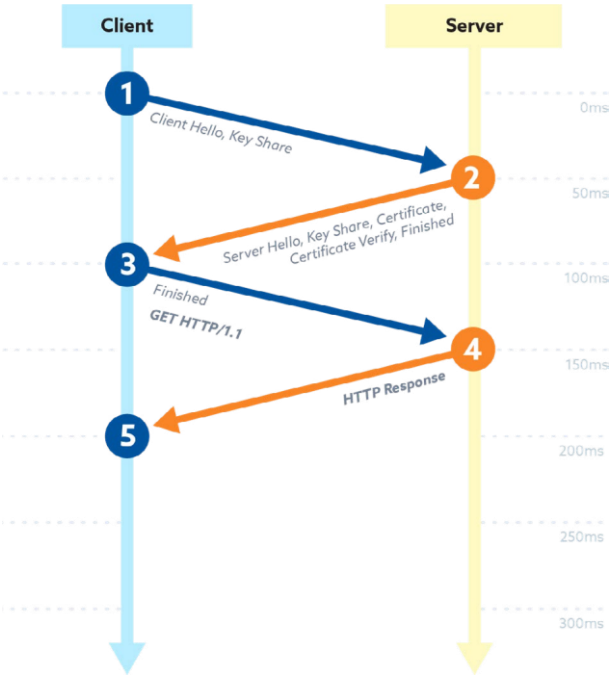

図4.TLS 1.3（フルハンドシェイク）

7.2.3 保存中の暗号化

データは、アプリケーション、ネットワーク、システム内で移動していない場合、「保存中」と考えられます。この「保存中」の期間にデータが適切に保護されていない場合、SaaSプロバイダのホスティング施設に不正にアクセスした攻撃者が、データを公衆に開示したり、営利目的で使用したりすることができてしまいます。この保存データの暗号化は、データを保存しているハードウェアが盗難に遭ってもそのデータを使用できないようにすることを確実にします。

また、データをアプリケーション自体において暗号化することで、SaaS利用者だけが自分のデータを見ることができますし（復号できるのはその利用者だけだから）、マルチテナントのSaaSプロバイダ環境での利用者間の境界線を提供することもできます。

暗号化のタイプと強度は、データの分類に依存します。保存されているデータが公共性の高いものと考えられる場合、高い機密性に分類されたデータほどの暗号化強度は必要ないともいえます。そのため、利用者組織は、SaaSプロバイダにデータを保存する前に、以下の点をレビューするべきです。

- データ流出に関するビジネスインパクト分析（BIA）
  - データを保存中に暗号化する必要があるかどうかを決定するために、組織はBIAを実施し、そのデータが公開された場合の影響を理解しなければならない。
  - さらに、データ漏洩のリスクを決定するために、アクセス管理など、CSPの他のセキュリティコンポーネントを考慮しなければならない。
- 保存中の暗号化サービスの利用可能性
  - すべてのSaaSプロバイダが、保存データの暗号化を無料サービスとして提供するわけではない。保存中の暗号化サービスを受けるために必要なライセンスモデルを理解します。
- 保存中のバックアップデータ暗号化の利用可能性
  - 多くのSaaSプロバイダは、保存中の暗号化を提供していますが、これはデータのバックアップには必ずしも適用されません。業務で使用する保存されたデータおよびすべてのバックアップの両方とも保存中の暗号化がなされることを確実にします。
- ディスク全体の暗号化vsファイルベースの暗号化の各手法の使用
  - 提供される保存中の暗号化のタイプを理解します。例えば、ディスク全体暗号化手法は、合理的な管理ですが、主にディスクやシステムが盗まれたときの保護に使われます。
  - より一般的なシナリオとして、ファイルベース暗号化方式の使用は、個々のファイルやデータを不適切なアクセスによる盗難から保護できます。
- 保存データの暗号化に使われる暗号化アルゴリズムと鍵長
  - 保存データの暗号化方式を確実なものとし、CSC のニーズを満たすようにする。NIST 800-57 第1部鍵管理に関する推奨事項 (表2を参考）に、アルゴリズムと鍵長に基づく暗号化強度の詳細が記載されています。

7.3 利用者管理暗号鍵 vs ベンダー管理暗号鍵

一般に、暗号鍵はベンダーから提供されるものより、利用者が管理するものの方が安全です。しかし、ベンダーが管理する暗号鍵を使用するかどうかは、2つの要因によります。まず、ベンダーは利用者が管理する鍵の使用を許可していますか。すべてのベンダーが、利用者の暗号鍵を使用する機能を提供しているわけではありません。第二に、ベンダーに保管されているデータが保証されているかどうか、また、ベンダーが管理する暗号鍵のリスクは許容できるか、です。

例えば、ベンダーが管理する暗号鍵を使用することによるリスクのレベルは、以下の質問に対する回答によって決まります。

- ベンダーは、暗号鍵の作成と管理方法について情報を提供していますか？
  - ほとんどの場合、ベンダーは自社環境における暗号鍵の作成とライフサイクル管理の詳細を共有することはないでしょう。
  - ベンダーの暗号鍵の作成と管理方法について安心感を得るために、データの転送中や使用中にどのようにデータが暗号化されるかについての文書を要求することをお勧めします。
- ベンダーのシステム内に保存されているデータの機密性はどの程度か？
  - 例えば、パブリックに分類されるデータは、ベンダー管理の暗号鍵を使用してもほとんどリスクがない場合があります。

- あなたの組織では、暗号鍵の管理はきちんとできていますか？
    - ベンダーのセキュリティに加え、鍵管理によって提供される保護は、利用者の組織におけるキーマテリアルの保護能力にも依存します。もし、あなたの組織がベンダーと比較して鍵管理の実行能力が未熟な場合は、ベンダー管理暗号鍵を使用することが得策かもしれません。

7.4 暗号・鍵管理の今後のあり方について

今後検討すべき分野

- HSMaaS（Hardware Security Module as a Service）
    - 「クラウドHSM」とも呼ばれ、SaaSで提供されるHSMを利用して暗号鍵を作成・管理する方法です。
    - まだ普及が進んでいませんが、FortanixやMicrosoftなど、FIPS検証済みのHSMaaSプロバイダが利用を増やしています。
- プライバシー拡張暗号（PEC）方式
    - システムが収集する個人情報や機密情報の量を最小限に抑えつつ、機能を維持するために使用される一連の技法。
    - SaaSプロバイダは、一般的なサービスを維持するために、PEC技術の利用をサポートしない場合があります。PEC技術は、結果を得るためにカスタマイズやユーザーシステムとの相互作用が必要になるからです。
    - NISTは、PEC技術を見直すためのブログ記事とプロジェクトを提供し、またPEC技術に関する規格や要件を作成しています。
- 準同型暗号
    - 使用中のデータを暗号化しつつ、ビットレベルでの暗号化・復号によりデータに対する操作を可能にします。従来の方法と比較して非常に遅い。
    - 準同型暗号を含むPEC方式に関する要求事項の文書化は、ISOやNISTなどの組織がオープンコンソーシアムを通じてリーダーシップをとり、現在も開発中です。
- 「コンフィデンシャル・コンピューティング」またはセキュア・エンクレーブ
    - ハードウェアに対応した機能を使用して、使用中のクラウドデータを他の作業ワークロードから分離して処理することで、データを保護すること。
    - NISTは、クラウドコンピューティングとエッジコンピューティングのための機密コンピューティング技術に関する詳細な情報を提供するドラフト文書を提供しています。
- ポスト量子暗号（PQC）方式
    - 少なくともまだ8年以上先の話だと思われます
    - 2016年のNIST内部報告書（IR）8105では、2000ビットのRSAを数時間で破ることができる量子コンピュータが2030年までに存在する可能性があると呼びかけています。
    - NISTやその他の組織では、ポスト量子暗号の標準化を目的としたプロジェクトや取り組みが進行中であり、そのうちのいくつかは、関連論文やフィードバックを公募しています。

8. 運用セキュリティ

8.1 運用手順と責任

8.1.1 文書化された業務手順

SaaS製品は柔軟性があるため、その製品が組織でどのように使われるかを理解する必要があります。

- アクセスコントロール - アクセスコントロールのセクションを参照
- 変更管理
- 容量管理
- 環境の分離
- 解約 - 解約のセクションを参照

8.1.2 変更管理

SaaS製品を追加する場合は、慎重に検討する必要があります。このような製品は、組織のエコシステムに簡単に追加できるため、問題を引き起こす可能性があります。そのため、強力な変更管理プロセスを導入する必要があります。SaaS製品では小規模な変更が頻繁に行われる傾向があります。多くの場合、その変化はユーザーには気づかれないかもしれませんが、下流のシステムに影響が出る可能性があります。

変更が組織のセキュリティポスチャに影響を与えるかどうかを特定することが重要です。組織は、ある変更により、他のシステムを修正する必要が生じるかもしれません。重要な変更、一般にはバージョンの変更ですが、変更管理プロセスの一部としてレビュー及び管理対象に含まれる必要があります。

さらに、SaaS製品は、特定の業務範囲のもとで使用されることが前提となっていることがあります。SaaSアプリケーションのその後のビジネス機能の変更、使用量の増加、使用の複雑さの変化により、SaaSアプリケーションの使用に付随するセキュリティの考慮事項を再検討する必要が生じることがあります。管理者は、SaaSアプリケーションの使用を定期的に見直し、最初のセキュリティレビューの範囲が現在の使用範囲と一致していることを確認することが推奨されます。これにより、SaaSアプリケーションの最新のセキュリティモデルを維持することができます。

8.1.3 容量管理

SaaS製品の使用には、ユーザー数に対するライセンス制限がある場合があります。また、モニタリング製品では、監視または添付されるアカウント数が制限される場合があります。ユーザー数またはアカウント数により、価格差が生じる場合があります。容量を増やす前に、ニーズを把握する配慮が必要です。

8.1.4 開発・テスト・運用環境の分離

社内開発システムと同様に、本番用データが本番用システムから流出しないよう、環境の分離が必要です。SaaSベンダーには、継続的なシステムの改良が求められています。改善、アップグレード、更新は、非本番環境と非本番データでテストする必要があります。SaaSベンダーは、別環境が存在することだけでなく、本番データがこれらの環境に存在しないことを証明する必要があります。

さらに、これらのSaaSアプリケーションの構成は、安全な環境が維持されていることを確認するために、継続的に評価する必要があります。ユーザーやサードパーティとの連携におけるセキュリティ設定やデータアクセスの誤りを特定することで、データ漏洩の発生リスクを軽減することができます。「ステージング->本番環境」のワークフローをサポートする環境では、ステージング環境でレビューを実施し、本番環境に影響を与える前にセキュリティ問題を特定できるようにする必要があります。

8.2 マルウェアからの保護

8.2.1 マルウェア対策

マルウェア対策に関する責任の大部分はSaaSプロバイダにありますが、SaaSユーザー/管理者の管理下にあるマルウェア配布の攻撃経路も依然として存在しています。これらのユーザー制御下の攻撃経路の例としては、カスタマイズ可能な静的ファイルのホスティングと添付ファイルがあり、SaaSアプリケーションを使用する組織の従業員/特権ユーザーのいずれかによって、またはSaaSアプリケーションが一般向けのポータルを提供している場合は一般ユーザーによってアップロードされる可能性があります。

SaaS管理者とそのセキュリティ組織は、典型的な脅威モデリングによる演習を実施し、SaaSの一般向け機能にコンテンツアップロード機能が存在する場合には、それを把握する必要があります。一般向けのコンテンツまたはドキュメントのアップロードシステムには、SaaSアプリケーションの内部または特権的なユーザーが会社のデバイスやその他のレビューが必要な機器にファイルをダウンロードしたり、保存または送信されたりすることを意図するものがあることに注意してください。

SaaSの導入と構成を評価する際、利用者はSaaSプラットフォームに組み込まれている機能を熟知しておく必要があります。多くの場合、マルウェアやウイルスのスキャン機能が標準装備されており、悪意のある可能性のあるアップロードにフラグを立てたり、ブロックしたりすることができます。SaaSシステムの構成は、（1）アップロード可能な外部制御コンテンツの種類と量を最小限に抑え、（2）内蔵の保護機能とファイルタイプの制限が有効になるように評価・監視する必要があります。

8.3 バックアップと高可用性

8.3.1 情報のバックアップ

多くのSaaSアプリケーションでは、データのバックアップ、冗長性、インフラやアプリケーション層の障害時におけるフェイルオーバーを管理する責任は、SaaSプロバイダにあります。SaaSの利用者は、データベースへの直接的なアクセスや、フェイルオーバー先のインスタンスやレプリカを作成する権限のようなものを持たないため、これは論理的な責任の割り当てになります。利用者によるデータアクセスは、SaaSプラットフォームが提供するAPIに限定され、一般的に、これらはデータのバックアップの作成や管理をするには、非効率的な手段です。壊滅的なデータ損失が発生した場合、SaaSプラットフォームのプロバイダがデータの復元に責任を負います。このため、SaaSの配備を管理する場合、情報のバックアップは、利用者が低いレイヤーを制御するIaaSなどの配備に比べると、重要な考慮事項ではありません。

そうは言っても、SaaS利用者が考慮すべき情報のバックアップに関する懸念は残っています。SaaSアプリケーションが想定および許容する範囲内で、不注意もしくは悪意によるデータ削除が行われた場合（例えば、悪意のある行為者が、サポートされている削除プロセスやAPIエンドポイントを使って、データやレコードを削除した場合など）は、SaaSプロバイダがバックアップの提供や復元に責任を持つことはありません。SaaSアプリケーションを利用者として管理する際の経験則として、プラットフォームが設計通りに動作している場合、たとえあなたの設定が誤っており安全でなかったとしても、SaaSプロバイダに問題を修正する責任はありません。

SaaS利用者として、このようなリスクを軽減するには、まず、データ損失を引き起こしかねない、不用意なアクセスや必要以上のアクセスがユーザーに付与されないようにするため、設定とデータアクセスの継続的な監視を導入することが重要です。これには、ユーザーに最小権限しか与えないようにデータアクセスを管理することや、論理削除やデータ保持の設定により、データの復元が容易になるようにシステム構成を監視することが含まれます。そして、SaaSプロバイダが、プラットフォーム上で「ロールバック」や「バックアップ」のソリューションをまだ提供していない場合、SaaS利用者は、重要データの冗長性のため、プラットフォーム外に、APIベースの追加のデータバックアップソリューションを導入するか検討する必要があります。

データのバックアップと併せて、CSCはスナップショットの戦略を実装する必要があります。NIST Standard 800-125では、スナップショットを次のように定義します。*「…実行中のイメージの状態を記録したもので、一般的に、あるイメージと現在の状態の差分として記録されます。例えば、スナップショットは、仮想ストレージ、仮想メモリー、ネットワーク接続、その他の状態に関連するデータの変更を記録します。スナップショットにより、シャットダウンや再起動することなく、ゲストOSを一時停止し、再開することができます。すべてではありませんが、多くの仮想化システムは、スナップショットを取得することができます。」*スナップショットの利点は、バックアップから復元するより短時間で、イメージやデータを復元できることです。

8.3.1.1 高可用性

多くのSaaSプロバイダは、SaaS利用者との契約においてSLAやOLAを定義しており、契約上の要件を満たせない場合には、サービスクレジットで補償することが多いです。つまり、SaaS利用者は、SaaSアプリケーションに求める要件に従って、他の冗長性のオプションを選択することもできます。SaaSが常に利用できるとは考えず、SaaSアプリケーションの可用性に問題が発生した場合のビジネス影響を考慮し、利用可能なオプションを検討することが必要です。

8.4 ログ出力と監視

8.4.1 イベントのログ出力

SaaSの配備におけるイベントログとアクセスログは、セキュリティチームがインフラや、IaaS、PaaS、アプリケーションのログで扱ってきた伝統的なログ出力の考え方とは、明らかに異なる課題を抱えています。SaaSアプリケーションのログを扱うセキュリティ組織の観点からは、SaaSアプリケーションを実行しているハードウェアやソフトウェアの下の層のログにアクセスできないという事実のため、大きな制約が存在します。SaaSアプリケーションの使用と管理を監視するセキュリティチームが扱うログは、定義上、SaaSプロバイダから提供されるログに制限されています。

まれに、より詳細なログや、より生の（アプリケーションのソースに近い）ログを、追加のコストと手動のリクエストプロセスによって、SaaSプロバイダから入手できる場合がありますが、そのような作業に関するタイムラグ、プロセスコスト、費用のため、SaaSのログ監視プログラムのベストプラクティスに含めるべきではありません。

SaaS アプリケーションのセキュリティを監視するセキュリティ組織にとっては、SaaSアプリケーションのログ出力に、業界標準として受け入れられたフォーマットが存在しないことが、状況をさらに複雑にしています。ユーザーのログインのような基本的なアクションでも、SaaSアプリケーションが異なれば、ログのメッセージフォーマットや内容が著しく異なる場合があり、SaaSアプリケーションを跨ってログやアクティビティを関連付けたいセキュリティ組織にとって、課題になります。

また、SaaSのイベントログをインシデント検知に利用したいセキュリティ組織にとって、ログが提供されるタイミングが課題となる場合があります。ログエントリーは、SaaSプロバイダによって処理され、APIやその他の配信機能を介して、エンドユーザーの自動アクセス向けに提供されるまで、SaaSアプリケーションのユーザーから利用することができません。SaaSプロバイダによる差はありますが、イベント発生からイベントログが利用可能になるまでのSLAは、数分から24時間までのどこかに規定されています。

これらの複雑さは、SaaSアプリケーションのセキュリティとアクティビティを監視できる唯一のメカニズムとして、SaaSのイベントログを使用する際の課題となりますが、SaaSセキュリティソリューションの一部として、SaaSのイベントログを監視することに価値がないわけではありません。SaaSのイベントログを扱うセキュリティ組織は、以下の機能を、開発または導入する必要があります。

- SaaSアプリケーションまたはプロバイダからのログ取得は、高い頻度で自動化します。

- SaaSのログは、SIEMや他のログ保管ソリューションに配信する前に、SaaSアプリケーション間で共通フォーマットに正規化します。これにより、セキュリティチームは、SaaSアプリケーションを跨ってアクティビティを効果的に監視することができます。
- イベント、監査、アクティビティ、およびその他のログエントリーが、ユーザー名やユーザーIDなどのユーザー情報を含む場合は、SaaSアプリケーション間でユーザー名やユーザーアカウントが異なっても、同一人物が行ったイベントを関連付けられるように、組織内で使っているアイデンティティに正規化します。
- SaaS アプリケーションごとに、アクションからログエントリーが利用可能になるまでの想定遅延、平均遅延、最大遅延を文書化し、ログシステムを使用するセキュリティ運用チームが理解できるようにします。

8.4.2 ログ情報の保護

8.4.2.1 管理者やオペレーターのログ

多くのSaaSアプリケーション、特に非常に複雑なアプリケーションでは、高い権限を持つユーザーによるシステムレベルの設定変更を監視するために、専用のログ出力や監査機能を備えています。このシステムは、「Audit Trail」や「Setup Log」と呼ばれることがあります。多くの場合、これらのログは、標準的なアクセスログやイベントログとは論理的に独立したデータ構造になり、取得するために別のAPIやアクセス方法を使うことがあります。

これらのログは、SaaSアプリケーションのセキュリティに重大な影響を与える可能性のある、特権によるアクションを記録するため、SaaSのイベント監視プログラムの一部として扱うことが重要です。これらのログも、この文書の「イベントのログ出力」セクションで概説されている、すべてのベストプラクティスに従う必要があります。

さらに、SaaSアプリケーションを監視するセキュリティチームは、一連のログの中で問題となるアクションの種類を特定し、これらのログを監視することにより、特権ユーザ（すなわち、SaaSの管理者）が行ったセキュリティに影響を与える変更を、セキュリティチームに警告する自動化されたセキュリティ技術の導入を検討する必要があります。SaaSのエコシステム全体で、これらの事前に定義した「高リスク」のアクティビティを監視することで、検知までの時間を短縮し、SaaSからのデータ漏洩による被害を軽減します。

8.5 技術的脆弱性の管理

SaaSアプリケーションの所有者を特定し、その所有者とセキュリティ部門との橋渡しを行います。多くの組織では、SaaSセキュリティは、エンタープライズセキュリティの責任範囲に含まれます。しかし、組織によっては、SaaSセキュリティを、アプリケーションセキュリティやサードパーティーリスクの問題と捉えることもあります。責任が誰にあるかにかかわらず、SaaSアプリケーションの所有者を特定し、各SaaSアプリケーションのビジネスユースケースを理解した上で、脆弱性管理の責任を定義することが重要です。

SaaSアプリケーションのセキュリティを統制することは、大きな課題です。例えば、SaaSの利用者は、SaaSプロバイダのインフラ内で発生した場合、SaaSアプリケーションの既知の脆弱性を軽減することができません。しかし、SaaSセキュリティにおける問題の大半は（そして、クラウドセキュリティの問題も同様に）、責任共有の利用者側で発生します。

この責任共有には、SaaSアプリケーションの設定と構成がセキュリティのベストプラクティスに沿っていることを管理することが含まれます。NIST CSF、ISO 27001、NIST 800-53などの標準に照らし合わせて設定を見直すことは、コンプライアンス違反や安全でない設定のリスクを低減するための強力なプラクティスです。

SaaSアプリケーションが脆弱なTLS暗号を受け入れる場合を考えてみましょう。利用者側のポリシーにより、このSaaSへの接続に、より耐性の高い暗号を使用するよう、すべてのユーザーに強制することで、この脆弱性が最終的に解決されるまでの間、影響を緩和することができます。さらに、管理者が重要なセキュリティ保護メカニズム（xss保護など）を無効にすることで、ユーザーにシームレスな体験を提供するシナリオを考えてみましょう。このシナリオでは、管理者は、継続的な監視メカニズムから設定ミスの警告を受け、問題を修正する必要があります。

8.5.1 技術的脆弱性の管理体制

SaaSセキュリティは、ITアプリケーションの所有者、エンタープライズセキュリティチーム、および技術部門のリーダーによる、部門横断的な協力を通じてのみ、最も効果的に改善することができます。ITアプリケーションの所有者は、問題への対策を行います。一方、セキュリティチームは、組織内で合意されたSLAの範囲内で対策が行われるように、トリアージとフォローアップを行います。他のセキュリティ領域と同様、承認された組織内のSLAに沿って、それに従うことが重要です。

クラウドセキュリティアライアンスのブログ記事「Building a SaaS Security Program: A Quick Start Guide」で詳細を説明しています。どのSaaSアプリケーションが、どのチームに属しているかを理解することが重要です。問題が特定された場合、適切なビジネスアプリケーションチームと会話をして、問題を解決する必要があるためです。ビジネスクリティカルなSaaSのワークフローに、最も緊急なセキュリティ問題が発生することは避けられません。

そのため、トリアージチームは、最も重要な問題を最初に修正できるように、すべてのセキュリティ脆弱性を棚卸し、それらを所有者に紐づけ、発見したリスクに対して重大度ベースの判断を下せるよう、迅速に行動する必要があります。

8.6 情報システム監査の留意点

8.6.1 情報システム監査の統制

SaaSプロバイダは、利用者の情報システム監査の管理下にないことがあります。しかし、利用者は、SaaSプロバイダが許容できるコントロールを整えていることの保証を（通常、規制によって）要求されます。これには、プロバイダの自己評価または第三者認証を使う場合があります。

自己評価は、法律に応えるための最低限のレビューではありますが、実施されているセキュリティ管理策が有効に機能しているかどうかを把握するには、最も信頼性の低い方法です。同様に、第三者認証のレビューでも、下記に注意して、慎重に読み込むことが肝要です。

- 評価のスコープ - 追加のIaaS、PaaS、SaaS、その他第四者のソリューションなど、評価のスコープに含まれない第四者がないか読み取ります。該当する場合、ベンダー管理やサードパーティーリスクのポリシー、インベントリ、評価が行われたスコープと深さを把握する必要があります。
- 検証と報告の方法 - オンサイトレビューを見送り、第三者評価（ISO 27001、SOC2 Type II）に頼る場合、熟練した確認者による徹底的な評価が必要です。できれば業界で認められた資格を持ち、理想的には、多層防御の戦略の実装経験を持つ確認者が望ましいです。
    - 第三者評価から、SaaSの技術やセキュリティ担当者へのインタビュー、ドキュメントのレビュー、サンプルの収集とテストが行われたことを確認できます。
    - 評価者の専門性は、報告書の文章から推察できることがあります。管理策の単純な言い直しとともに「除外事項」と記載され、テスト方法の記述がない、もしくは不明瞭な記述の場合、その内容は使うべきではありません。

この課題は、SaaSプロバイダが受け入れ可能な特定の基準（CSAのCCM、FedRamp、NIST、ISOなど）に従うことを求め、それらの基準に対する認証と、管理策の有効性を示す成果物の定期的なレビューの提供を契約条項に含めることで解消できるかもしれません。

クラウドセキュリティアライアンスは、Auditing Guidelines based on Cloud Controls Matrix (CCM) version 4を提供しています。このガイドラインは、CCMによる監査をガイドすることを目的としています。監査人は、CCMv4.0の管理策の仕様ごとに評価ガイドラインを提供され、これらは、管理策の実装の可監査性を向上させ、組織がより効率的にコンプライアンスを達成できるようにすることを目的としています。このガイドラインは、網羅的でも規範的でもありません。評価のための推奨事項をまとめた一般的なガイドです。監査人は、監査の特定の目的に対応するため、説明、手順、リスク、管理策、文書などをカスタマイズし、評価スコープの組織やサービスに対する監査作業プログラムに合わせる必要があります。

9. ネットワークセキュリティマネジメント

SaaSサービスの利用におけるネットワークセキュリティやデータフロー・セキュリティに関連する管理のガバナンスは、SaaSプロバイダが所有・運営する管理と、SaaS利用者が考慮する必要がある管理の2つの領域に分類されます。

両ドメインにまたがる重要なネットワーク制御は、転送中のデータの暗号化、特定のリソースへの権限付与、データ転送制御などに要約されます。

ここでは、ネットワークセキュリティに対する「Zero Trust Network Access」と「Secure Access Service Edge」のアプローチについて解説しています。

9.1 SaaSプロバイダのネットワーク制御

サービス利用者は、外部接続とマイクロサービスの内部保護に有効なTLS証明書が利用されていることをSaaSプロバイダに確認する必要があります。証明書は、よく知られた信頼できる認証局からのものであるべきで、自己署名されたものであってはなりません。

さらに、サービス利用者は、SaaSプラットフォーム内の個別のサービスコンポーネント間で、どの程度まで暗号化が利用されているかを確認する必要があります。

SaaSプロバイダは、最小特権ベースのゼロトラストネットワークアクセスポリシーによって、ネットワークデータの流れを制御することができます。SaaSプロバイダは、検出制御としてネットワークフローの異常検出機能を利用することができます。

9.2 SaaS利用者ネットワークの管理策

サービス利用者は、SaaSプロバイダのセキュリティ態勢とリスクを評価する際に、以下のネットワークセキュリティ管理を考慮する必要があります。

SaaSプロバイダへの接続は公衆インターネットを経由することがあるため、TLS 1.2+などの暗号化によって転送中のデータを保護することは、重要なセキュリティ管理です。

SaaSサービスへのアクセスは、SaaS利用者が管理していないアカウントにデータをアップロードすることで、悪意のある行為者がデータ流出を行う機会を生み出す可能性があります。クラウドアクセスセキュリティブローカー（CASB）とテナンシーチャンネルの認証制御を使用して、このリスクを制御します。

データ漏洩対策（DLP）も考慮する必要があります。DLPは、ペイロードデータへのアクセスに応じて、ネットワークまたは他のレイヤーに導入されます。

サービス利用者は、SaaSプロバイダとのネットワーク接続を構築する際に、インターネット回線の冗長化やキャパシティプランニングなど、可用性の要件を考慮する必要があります。

SaaSの利用者は、Protective DNS（多くの場合、SaaSベースのサービス）によるDNSトラフィックの制御を考慮する必要があります。
現代のネットワークアーキテクチャは、アウトバウンドのインターネットアクセスの分解を活用し、ローカルブランチのインターネットブレイクアウトをもたらす可能性があります。SaaS利用者は、利用者がSaaSサービスを直接利用する場合、上記のような管理の適用を考慮する必要があります。

セキュアアクセスサービスエッジ（SASE）モデルは、SaaS利用者とプロバイダの間のポリシー実施ポイントとして機能することで、この制御態勢を促進することができます。

10. サプライヤーとの関係

10.1 サプライヤーとの関係における情報セキュリティ

SaaS製品は、ほとんどの場合、サードパーティのサービスの上に構築されており、サプライヤーが直接管理・保守するものだけでなく、第四者であるIaaS、PaaS、SaaSの提供するものも含まれます。従来の顧客管理型ソフトウェアとは異なり、SaaSの利用者は、当該製品が依存する完全な依存関係を理解することが困難な場合が多いです。そのため、SaaS製品を運用する企業は、自社のビジネスオペレーションが依存するテクノロジーの包括的なモデルを構築することが重要です。

従来の顧客管理型ソフトウェア展開と同様に、SaaS提供のためのソフトウェア部品表（SBOM）（SaaSBOMとも呼ばれる）を開発することで、このようなモデルを提供することができます。既存の規格CycloneDXは、SaaSコンポーネントを組み込んだSBOMの作成を容易にすることができます。SBOMを評価することで、企業はテクノロジーのサプライチェーンにおける脆弱性を特定し、より迅速に修正することができます。

SaaS製品を構成するコンポーネントをリアルタイムで把握・管理することに加え、SaaS製品を利用する際の内部リスク管理方針を策定する必要があります。同様に、企業は、提供するサービスのセキュリティを確保するために、CSPと契約条件を交渉する必要があります。最後に、外部認証制度は、リスクマネジメントの分析・判断に役立ちますが、SaaSサービスを利用する組織は、それだけに依存するべきではありません。

10.1.1 サプライヤーとの関係における情報セキュリティポリシー

事業運営の一部を他者に依存しているすべての企業、つまり現代経済では基本的にすべての企業が、サードパーティーリスクマネジメントポリシーを導入する必要があります。組織が直接関係を持つ第三者だけでなく、これらの外部関係者は、それ自体が第四者との関係や依存関係のネットワークを持つことになり、第三者リスク管理方針が必要になります。

このポリシーは、組織が依存する他のテクノロジーに加え、SaaS製品にも適用される必要があります。このようなポリシーは、最低限、以下の項目を特定する必要があります。

- 第三者との関係（およびそれに内在するすべての第四者リスク）に対して、組織内で説明可能な単一の役割または立場。
- 第三者の製品またはサービスに依存する業務運営の重要性について、できれば定量的に、その役割または立場を担う人物が書面による評価を提供することを要件とします。
- 上記で特定した重要性を考慮し、事故がそのような第三者に影響を与える可能性及びそのような事故が組織の業務に与える影響を評価するための方法論。これは以下の利用を含みますが、これらに限定されるものではありません。
    - 外部監査およびセキュリティレビュー (詳細は認証保証の項を参照)

    - セキュリティスコアリング/評価ベンダーのツール
    - 顧客組織による監査、侵入テスト、プロバイダの製品またはインフラに対する自動スキャンツールの使用など、直接的な技術的デューデリジェンス
- 上記に基づいて設定されたリスク閾値は、第三者がこれを超えた場合、第三者側（契約で義務付けられている）、組織自体（何らかの補償的管理を通じて）、またはその両方による是正措置の要求の引き金となるものです。
- 上記の閾値を超えるリスクを受容する権限を有する、組織内の単一の説明可能な役割又は地位、並びにそのようなリスク受容を文書化し正当化するための透明性のあるプロセス

10.1.2 サプライヤー契約におけるセキュリティへの対応

サプライヤーとの契約では、SaaS製品の安全かつ信頼性の高い運用を確保するための様々な対策を求める必要があります。SaaSプロバイダは、さまざまな規模や複雑さの組織を代表しており、その提供物の組織にとっての重要度もさまざまでしょう。そのため、個々のサプライヤーに合わせた契約書の作成が必要になる場合があります。このような契約には、以下のようなものがあります。

- 製品の可用性（アップタイム）だけでなく、基礎となるデータの機密性と完全性についてのサービスレベル合意書（SLA）。例えば、インセンティブを適切に調整するために、組織はベンダーに対して、悪意のある行為者によって公開または破損された特定の種類のレコードごとに所定の手数料を支払うことに同意するよう求めることができます。
- 組織が監査や侵入テストなどの外部検証プロセスを受け、その結果を提供することを要求します。
- 客観的なリスク評価システムに基づいて、組織が特定した脆弱性（ただしサプライヤの製品に存在するもの）を、所定の期間内に解決または緩和策を特定する要求事項。
- 組織が脆弱性の重大性または悪用の可能性を低減するための代償措置を適用できる脆弱性を供給者が特定した場合，供給者は特定の期間内に組織に通知するという要求事項。
- 組織のデータの機密性、完全性、可用性に影響を与えた、または与える可能性のあるインシデントの調査及び是正において、供給者が組織に協力するための要求事項。
- データセンターの新規立地を通知し、好ましくない立地を拒否する権利を供給者に求める要件

サプライヤーと交渉する組織は、リスクマネジメントに慎重に焦点を当て、契約に有償の条件を追加することは避けるべきです。例えば、サプライヤーのネットワーク、システム、ソフトウェアに脆弱性が発見された場合、それを組織に通知するよう求めると、警告が殺到し、対策を講じる上で本質的に役に立たないことが予想されます。

10.1.2.1 外部認証

外部認証は、プロバイダが特定の要件を満たしていることを、信頼できる外部組織が証明するものです。このような証明書は、CSPのリスク評価を行う際に役立ち、プロバイダが主張する管理体制と実際のセキュリティポスチャを明確にするのに役立ちます。とはいえ、外部認証の審査は、包括的で広範な第三者リスク管理プログラムの代わりではなく、補完的なものであるべきです。

すべての認証や監査報告書が同じであるわけではなく、また同じ種類の報告書が同じ範囲をカバーするわけでもありません。ISO/IEC 27001などの認証は、CSPが、所定の管理セットに従って情報セキュリティ管理の基本水準を確立していることを示します。

SOC 2監査証明は、プロバイダが確立した統制を遵守する能力を監査人が評価することに基づいています。ただし、ISO/IEC 27001とは異なり、SOC 2報告書それ自体は「認証」ではありません。 監査人は、監査範囲となるTrustサービス基準（プロバイダが選択）に対して、プロバイダがこれらの基準の要件を満たしているかどうかについて、4種類の意見のうちの1つを表明します。また、監査人の報告書には、プロバイダが実装していると主張しているコントロールについて特定された除外事項も記載されます。多くのベンダーは「SOC2準拠」を主張しますが、これは監査の結果ではありません。SOC2報告書を確認する場合は、必ず以下の点を確認してください。

- どのTSP基準（セキュリティ、機密保持、可用性、処理のインテグリティ、プライバシー）を考慮したのか。
- 報告書のタイプは以下のどれか
  - SOC 2 Type1 - 受託会社のシステムとTrustサービス基準に基づく内部統制のデザインについて示します。報告書には、現在のシステムとコントロール及びこれらのコントロールに関連する文書に対して実施されたレビューが記載されます。すべての管理的、技術的、論理的なコントロールの設計の検討は、特定の時点で検証されます。
  - SOC 2 Type 2 - サービス組織のシステムが関連するコントロールをデザインし、適用しており、それらのコントールが有効であるか否かを示します。SOC2 Type2の監査は、導入されたシステムやコントロールがサービス組織の経営者が言明しているように機能しているかどうかを、最低6カ月間、証拠を収集し、分析することで実施されます。通常、SOC 2 Type 2 の報告書はMNDA（双務的秘密保持契約）により共有されます。
  - SOC 3 - これはSOC2 Type2報告書に類似した、一般に共有可能な報告書です。
- 独立監査人のコメントセクションを必ず読んでください。監査人は、どの部分が非準拠であるかを示します。これにより、SaaSプロバイダがポリシーや手順で述べていることを実践しているかどうかを知ることができます。

どのCSPの報告書を見るにしても、認証または監査証明の範囲と事業主体に細心の注意を払うことが肝要です。範囲は、検討または利用するSaaSサービスを対象とし、事業主体は、契約を締結する相手である必要があります。例えば、ベンダーによっては、自社の内部統制を検証した報告書ではなく、自社のサービスが稼働しているIaaSプロバイダのSOC 2 監査証明報告書を提供する場合があります。第四者リスクの分析には有用であるものの、このような報告書はプロバイダ自体のレビューに代わるものではありません。

同様に、アプリケーションを収容するデータセンターだけでなく、組織が依存するサービス全体をカバーしているかどうかを判断するために、報告書を確認する必要があります。

以下は、SaaS利用者がCSPのセキュリティを評価する際に利用できる保証報告書、証明書、および認証の非包括的なリストです。

- 包括的
  - 米国公認会計士協会（AICPA） - SOC 2
  - 国際標準化機構（ISO）／国際電気標準会議（IEC） - 27001
  - HITRUST - Common Security Framework（CSF）
- 政府主導
  - 米国 - FedRAMP
  - シンガポール - SS584
  - 欧州連合 - EU 一般データ保護規則（GDPR）
- クラウドセキュリティに特化
  - Cloud Security Alliance - STAR
  - ISO/IEC - 27017
- 金融取引に特化
  - BSI Kitemark - Secure Digital Transactions
  - Payment Card Industry - DSS
- プライバシーにフォーカス
  - ISO/IEC - 27018

11. インシデント管理

11.1 クラウドを主として採用している場合の情報セキュリティインシデントの管理

多くの企業がクラウドファーストを掲げています。このような組織は、よりビジネス主導の決定がなされることが多いものの、情報セキュリティの基礎となるプロセスや手順を適宜見直し、適合させ、採用しなければならないことを認識する必要があります。その重要な文書の一つが、セキュリティあるいはサイバーインシデント対応（IR）計画です。健全なセキュリティガバナンスの一環として、既存のIRプロセスおよび手順を見直し、ビジネスで活用されるすべてのクラウドコンピューティングサービスおよび配備モデルを組み込む必要があります。

クラウドインシデント対応の詳細と各フェーズについては、CSAのCloud Incident Response Frameworkを参照することを強く推奨します。

11.2 Software-as-a-Service インシデントレスポンスの責任と手順

業界内でしばしば誤解されているように、デジタル情報資産をクラウドに移行しても、責任（ただし、マネージドサービス契約の文脈で明確な契約上の合意があれば例外が存在します）や説明責任が完全に移行するわけではありません。最終的には、資産（およびその上に存在するデータ）の所有者が、さらされたリスクに見合ったデューケアを行いながら、資産を管理することに全責任を負います。クラウドコンピューティングの3つのサービスモデルのうち、Software-as-a-Serviceモデルは、他のモデル（PaaSとIaaS）と比較して、クラウドサービス提供者が最も責任を負うモデルです。CSAのセキュリティ・ガイダンスv4にあるように、SaaSでは、ほぼすべてのレイヤーのセキュリティにクラウドプロバイダが責任を負うことになります。クラウドサービス利用者（CSC）が管理できるのは、アプリケーション（クライアントデバイスを含む）のIDとアクセス、アプリケーションの情報クリアランス、プロバイダによってはデータの暗号化設定（Bring your own keyなど）だけです。CSC は、仮想化、ネットワーク、周辺セキュリティを管理することができません。Centre for Internet Securityによる責任共有モデルのイメージをご参照ください。

責任	オンプレ	IaaS	PaaS	SaaS	FaaS
データの分類と説明責任	●	●	●	●	●
クライアントおよびエンドポイントプロテクション	●	●	●	●●	●●
アイデンティティとアクセス管理	●	●	●●	●●	●●
アプリケーションレベルのコントロール	●	●	●●	●●	●●
ネットワーク制御	●	●●	●	●	●
ホストインフラ	●	●●	●	●	●
物理的なセキュリティ	●	●	●	●	●

● クラウド利用者が責任を負う　● クラウドプロバイダが責任を負う　●● 責任の共有

このモデルでは、技術的な責任が一部移行されるため、企業のセキュリティ要件や標準的なベースラインに合致した、明確な契約上の合意をクラウドサービスプロバイダと結ぶことが不可欠となります。CSCは、この議論を促進するために、調達段階においてCSA Consensus Assessment Initiative Questionnaireを活用することができます。前述したように、CSCはどのような状況であっても、企業の情報および資産を保護する責任を負っています。責任は移せますが、説明責任は移せません。

利用者のインシデント対応計画は、これらの技術的制約を取り入れるために更新され、重要なCSPの連絡先の登録を維持しなければなりません。セキュリティおよび非セキュリティインシデントに関するサービスレベル合意書は、契約書を通じて合意されなければなりません。

11.3 フェーズ 1:準備

CSA Cloud Incident Response frameworkで説明されているように、準備のレベルは、組織が（サイバー）セキュリティイベントにどのように対応するかに直結しています。SaaSサービスについては、企業（公認）のSaaSランドスケープをしっかり理解することが必要です。すべてのSaaSサービスは、調達プロセスにおいて吟味され、企業のリスク選好度、規制や業界のコンプライアンス要件に沿った、信頼できる第三者のリスク分析が含まれる必要があります。CSCが直接（技術的に）管理していない特定されたリスクは、評価され、必要であれば、契約により軽減されなければなりません。

CSCは、このサービスの重要性を、サプライチェーンのリスクと事業目的の継続性（機密性、完全性、可用性の評価）の観点から理解することが最も重要です。次に、調達したSaaSサービスについて、重要なステークホルダー（ビジネス、技術（IT/ITセキュリティ））の連絡先のリストを文書化し、中央の企業資産データベースに追加し、インシデント対応者（またはCSIRTの他のメンバー）が知っている必要があります。

SaaSに特化したプレイブックは、このサービスモデルに適用される脅威/不正使用のシナリオに合わせて作成される必要があります。SaaSプロバイダが侵害された場合、企業（社内/社外）のステークホルダーに知らせるためのコミュニケーションの文案を準備することができます。影響がまだ明確でない、または完全に完了していない場合でも、利用者/パートナーに積極的に通知するためのステートメントを発行することができます。SaaSサービスごとに一元的に保存されたパラメータやタグ（たとえ

ばCMDB：構成管理データベース）があれば、どのようなコミュニケーションを行うべきか（例：テナントが一般消費者の個人データを管理しているかどうか）を判断するのに有益です。

11.4 フェーズ2:検出と解析

利用者（CSC）はデータとデータへのアクセスの保護にのみ責任を負うため、このようなSaaSコンテキストにおけるインシデントのほとんどは、CSPが所有するシステムによって検知されます。ただし、IDプロバイダのシグナルやSaaSサービスのアクセスログを活用することで、不正なアクセスを注意深く監視する必要があります。CSCは、データの流出や偵察活動（ハニートークンの使用）を検知することに全責任を負います。このため、CSCは、多要素認証を含む企業のアイデンティティ・プラットフォームとSaaSサービスの統合を常に目指していかなければなりません。次に、CSPから発信されるアラートを標準的なCSCのインシデント対応プロセスと組み合わせる必要があります。好ましくは、アラートを自動的に取り込み、適切な優先順位を割り当てることによって自動化することです - SaaSサービスがビジネスクリティカルかどうかによって直接的に影響を受けます。CSPがサポートしている場合、ログはCSCのSIEMまたはIDSソリューションにオフロードされる必要があります。

後者とは無関係に、確立されたSaaS CSPの関係者契約を活用して、合意された契約上のサイバー条項を発動し、機密性、完全性、可用性の潜在的な侵害を分析するために必要なサポートを得ることが依然として重要です。最後に、フォレンジック調査には、CSPの関与が不可欠となります。

4.1フェーズ3:封じ込め、根絶、回復

これまでのすべてのフェーズと同様に、CSCは対応の動作に制約があります。CSCができることは、発信元IPに基づくテナントへのアクセス制限（注：すべてのSaaSプロバイダが対応しているわけではありません）、ユーザーやアカウントのアクセス権の取り消し（OAuth許可、鍵ローテーション、多要素トークンなどを含む）、データ保存時の暗号鍵のローテーションなどのみとなります。

復旧に関しては、CSPに必要なサポートを依頼し、CSCのデータバックアップと復旧計画を発動させることが重要です。これは、CSCがサードパーティ製のバックアップツールを活用するか、CSPにテナントデータの復元を依頼することで実現できます。

4.2フェーズ4:事後分析

深刻な危機を決して無駄にせず、一歩下がって学んだ教訓を見直すことは、健全なIRPとしての重要な最終ステップです。インシデントを見直し、プランのどの要素を改善できるかを判断します。技術的なものから、管理的なもの（SaaSプロバイダとの契約上の合意事項の見落としや、プロセスのステップの見落としなど）まであります。主な質問としては、以下のようなものが考えられます。

- イベントの検出は間に合ったのか、それとも改善できるのか？(メトリクスとログ)
- ベンダーから必要なサポートが得られたか？(契約/SLA)
- ステークホルダーに適切なタイミングで情報を提供したか？（コンプライアンスとコミュニケーション）

この事後報告の結果は、フェーズ1の教訓として直接フィードバックされ、CSCが（SaaS）インシデントをよりよく管理するための準備に役立つはずです。事故後の分析は、単に時系列や事象を整理するだけでなく、学習プロセスであることが理想的です。この優れた例として、厳密にセキュリティに焦点を当てたものではありませんが、Jeli、Netflix、Slack、Adaptive Capacity labsが元々共同で作成した「how we got here」または「howie」プロセスが挙げられます。

あるいは、事故後の情報が同業者や他のCSPに利益をもたらすかどうかを評価する必要があります。関係者に向けて告知メッセージを発表したり（2021年11月16日のGoogle Cloudの障害の例を参照）、CSAのCloud Cyber Incident Sharing Center（CloudCISC）を活用することも選択肢の一つです。情報共有や連携の指針として、CSA Cloud Incident Response Frameworkの第6章をご参照ください。

12. コンプライアンス

12.1 セキュリティポリシー・基準の遵守

機密データを保存・処理するためのSaaSアプリケーションの使用は、他のすべての企業システムと同じ方法で、同じ厳しさで、関連するすべての社内外の適用されるコンプライアンス基準やセキュリティポリシーに対して評価されなければなりません。特に、SaaSアプリケーションは、その中に含まれるデータの種類と機密性に加えて、リスクにさらされる記録の数、組織の信頼性、継続性などの関連するリスク要因に基づいて分類・評価されるべきであることを意味します。

遵守している組織は、少なくとも以下を理解し、文書化し、監視する必要があります：

- SaaSアプリケーション内のデータの関連する分類
- SaaSアプリケーションに広範にアクセス可能なユーザーの種類。
- SaaSアプリケーション内の各データ分類に対してアクセスすることができるユーザーの種類
- SaaSアプリケーション内で実施されているアクセス制御について
- SaaSアプリケーションで利用可能なあらゆる監査機能
- SaaS利用者に関連する、適用可能な準拠フレームワークのコンプライアンス評価または証明書

特に、機密データやコンプライアンス関連データを含み、かつ 外部（非従業員や非特権ユーザー）にポータルやその他のエントリポイントを公開しているSaaSアプリケーションを使用する場合は注意が必要です。これらのSaaSアプリケーションは、設定を誤るとコンプライアンス要件から最も大きく逸脱する可能性があるため、特に慎重な調査と監視が必要です。例えば、匿名のインターネットや不正なユーザーへのデータ流出などです。

多くの組織では、SaaSアプリケーションのコンプライアンス評価と認証は、通常は四半期または年1回など、必要に応じて行われますが、セキュリティとコンプライアンスの両方のニーズを満たすことができる自動化された継続的なモニタリングシステムを導入することがより効果的です。
継続的なモニタリングシステムを構築するための必要となる労力は、一般的に、コンプライアンスサイクルにおいてコンプライアンスを一度検証するために必要な労力と同等であると言われています。継続的なモニタリングシステムは、将来のコンプライアンスサイクルにおける労力を削減し、システムがコンプライアンスから外れる可能性のある時間を短縮するため、長期的な投資として価値があるものです。また、従来のスナップショット的な評価活動ではなく、ほぼリアルタイムでのコンプライアンス保証が可能になります。

このような継続的なモニタリングソリューションの導入には、一般的に以下のようなものが必要となります：

- 各コンプライアンスフレームワークの範囲に含まれる、あるいは関連する、SaaSアプリケーションを特定する。
- 関連する各SaaSアプリケーションのどのユーザーグループや群を、監視対象とするか、コンプライアンス上の懸念事項であるかを特定する
- 関連するコンプライアンスフレームワークによって要求されるSaaSアプリケーション固有の設定やアクセス制御を、それらが満たすフレームワークの要素にマッピングする
- ソフトウェアベースのツールを利用して、SaaSアプリケーションの自動化された継続的なモニタリングおよびレポートアクティビティを促進する

これらの取り組みが完了し、継続的なモニタリングソリューションが導入されれば、SaaSアプリケーションとそのデータが、関連するすべての内部標準と外部のコンプライアンスフレームワークに準拠していることを確認することは、ほぼ自動化されたプロセスとなります。この継続的なモニタリングを利用して、必要に応じて成果物を生成し、SaaSアプリケーションがコンプライアンスに準拠していること、および所定の期間にわたってコンプライアンスに準拠していたことを検証することができます。

独自のデータ保持期間を要求することは、契約段階で交渉するのがベストです。カスタムタスクを完了するためにSaaSソリューションを調達した場合、処理したデータをSaaSソリューションから永久に削除できるのはいつですか？SaaSソリューションにデータ保持の法的義務がある場合、処理されたデータをオフラインストレージに一定期間転送することができますか？カスタムリテンションタイムをリクエストすることで、大幅なリスク低減が可能です。

12.2 法令・契約上の要求事項の遵守

12.2.1 適用される法律および契約上の要求事項の特定

「サプライヤーとの関係」セクションの「サプライヤー契約におけるセキュリティへの対応」を参照してください。

12.2.2 知的財産権

クラウドの利用者は、CSPのプラットフォームの使用に関する「利用規約」を確認し、理解する必要があります。場合によっては、CSPは利用者データにアクセスする権利を留保することができます。また、CSPは、特定の業務について、第三者であるベンダーと契約することがあります。また、クラウドの利用者のデータに外部の企業がアクセスする可能性もあります。

12.3 情報セキュリティレビュー

上述したように、継続的なモニタリングツールや手法を活用することで、組織のSaaS利用に対する情報セキュリティレビュー活動を促進することができます。これらのレビューは、コンプライアンス評価、組織や業界のセキュリティベストプラクティスの遵守、十分なセキュリティ衛生の実施などの活動で構成されることがあります。情報セキュリティレビューには、組織のSaaSインベントリを評価し、認可されていない可能性のあるSaaSの利用を特定する活動も含めるべきです。

13. CASBの機能と今後の展望

クラウドアクセスセキュリティブローカーは、SaaSサービスの普及に伴い、シャドーIT（企業のIT部門が認可していない、つまりセキュリティが確保されていないサービス）の可視化、監視、制御に焦点を当てた重要なカテゴリの1つです。主な機能は以下のとおりです。

- リスクについての洞察：最初のユースケースは、クラウド利用者のデバイスからのデータ転送のログと共に利用者のデータを、個々のクラウドサービスに関するリスクについて分析し、次のような洞察を共有することでした。
  - 利用者環境におけるクラウドサービスの総数
  - リスクの高いサービスの割合（例：リモートデスクトップコントロール、コラボレーションアプリケーションなどのアプリケーションカテゴリ）
  - リスクの高いクラウドサービスにアップロードされるデータの量
  - 購入することが許可されていないアプリケーションを判断するために、会社のクレジットカードを利用して取得されたクラウドサブスクリプション

この可視性は、ビジネスの意思決定者にとって予期せぬものでした。次の質問は、もちろん、今見えているリスクのコントロールについてです。

- API： このモードは、APIを活用して、さらに可視化と制御を行います。一般的なユースケースとしては、例えば、最大のデータ量をダウンロードしている上位ユーザーをリストアップすることや、企業データの特定のサブセットに対する外部からのアクセスを禁止することなどが挙げられます。このモードで行われるすべてのポリシーアクションは、ほぼリアルタイムです。
- インライン： このモードでは、アプリケーションのトラフィックを実際にCASBクラウドに誘導し、トラフィックパターンを解読してアップロードやダウンロードなどの特定のアクティビティを検出し、従来の許可またはブロックポリシーではなく、きめ細かいポリシーを適用することで、最も包括的なカバレッジを提供します。よくある例としては、リスクが中程度のクラウドアプリケーションに対して、データ保護ポリシーに違反しないダウンロードのみを許可するポリシーが挙げられます。

SaaS Security Posture Management (SSPM)は、SaaSアプリケーションをCISやNISTなどの業界標準にマッピングされた事前定義されたポリシープロファイルに照らして継続的に監視し、SaaSアプリケーションの構成管理を簡略化および自動化するもので、新たな関連カテゴリです。設定ミスはすぐに警告され、ユーザーは悪用される前に問題を自動的に修正することも可能です。

これらのカテゴリは進化を続け、Secure Services Edge（SSE）という新しいカテゴリに収斂されています。この進化の詳細な分析は本稿の範囲外ですが、クラウドやSaaSのセキュリティ担当者は継続的に追跡しておくべきことです。

14. 結論

SaaSの活用は加速する一方であることは明らかです。この加速に伴い、企業がクラウドサービスを運用・利用する方法にも大きな影響が及んでいます。しかし、従来のクラウドセキュリティとは異なり、SaaSの場合はそのニュアンスが異なるため、さらなる注意と対処が必要です。これには、組織が情報セキュリティポリシー、アクセス管理、アクセス制御をどのように扱うかが含まれます。データがもはや利用者の管理下にないため、暗号化と鍵の管理に関する考察が最も重要になります。ネットワークセキュリティに対する決定は、利用者がSaaSサービスにアクセスする方法と、プロバイダからSaaS利用者の組織環境（オンプレミスかクラウドかにかかわらず）に接続する可能性の両方に影響する可能性があります。また、SaaSは、SaaSベンダーだけでなく、基盤となるクラウドやホスティングのプロバイダから構成されることが多く、複雑なサプライチェーンとなっています。インシデント管理と事業継続の方法は、SaaSがビジネスオペレーションに果たす役割の増大を考慮し、見直す必要があります。

SaaSは、企業が業務方法を変更し、革新的な機能を利用し、アプリケーションの作成と保守の両方に関連する多くの運用負荷を軽減するための多大な機会を提供しますが、懸念事項がないわけではありません。これらの懸念に対処しない場合、SaaSの利用に関連するセキュリティインシデントの潜在的なリスクと影響が増大する可能性があります。

15. 参考文献

Cloud Security Alliance. (n.d.). Security, Trust, Assurance and Risk (STAR). CSA. Retrieved May 20,2022, from https://cloudsecurityalliance.org/star/

Cloud Security Alliance. (2017, July 26). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. CSA. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Cloud Security Alliance. (2021a, May 4). Cloud Incident Response Framework. CSA. https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/

Cloud Security Alliance. (2021b, June 7). Cloud Controls Matrix and CAIQ v4. CSA. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

Cloud Security Alliance. (2021c, June 7). STAR Level 1: Security Questionnaire (CAIQ v4). CSA. https://cloudsecurityalliance.org/artifacts/star-level-1-security-questionnaire-caiq-v4/

Cloud Security Alliance. (2021d, July 29). Cloud Threat Modeling. CSA. https://cloudsecurityalliance.org/artifacts/cloud-threat-modeling/

Cloud Security Alliance. (2021e, December 8). CCMv4.0 Auditing Guidelines. CSA. https://cloudsecurityalliance.org/artifacts/ccm-v4-0-auditing-guidelines

International Standards Organization. (2020, December 16). ISO/IEC 27001:2013. ISO. Retrieved May 20, 2022, from https://www.iso.org/standard/54534.html

International Standards Organization. (2021, April 15). ISO/IEC 27002:2013. ISO. https://www.iso.org/standard/54533.html

International Standards Organization. (2022a, February 4). ISO 31000:2018. ISO. https://www.iso.org/standard/65694.html

International Standards Organization. (2022b, May 4). ISO/IEC 27000:2018. ISO. https://www.iso.org/standard/73906.html

16. 定義

クラウドアクセスセキュリティブローカー（CASB）。クラウドサービス利用者とクラウドサービスプロバイダの間に設置され、クラウドベースのリソースにアクセスする際に、企業のセキュリティポリシーを組み合わせたり差し込んだりするオンプレミスまたはクラウドベースのセキュリティポリシー実施ポイントです。CASBは、複数の種類のセキュリティポリシーの実施を統合します。セキュリティポリシーの例としては、認証、シングルサインオン、認可、クレデンシャルマッピング、デバイスプロファイリング、暗号化、トークン化、ロギング、アラート、マルウェア検出／防止などがあります。[1]

SaaS（Software as a Service）。利用者に提供される機能は、クラウドインフラ上で動作するプロバイダのアプリケーションを使用することです。アプリケーションは、ウェブブラウザなどのシンクライアントインターフェース（ウェブベースの電子メールなど）、またはプログラムインターフェースのいずれかを介して、さまざまなクライアントデバイスからアクセス可能です。利用者は、ネットワーク、サーバー、オペレーティングシステム、ストレージ、あるいは個々のアプリケーションの機能など、基盤となるクラウドインフラを管理・制御しません。ただし、ユーザー固有のアプリケーション構成設定については例外となる場合があります。[2]

ソフトウェアの部品表（ Software Bill of Materials ）。ソフトウェアを構築するために使用される様々なコンポーネントの詳細とサプライチェーンの関係を含む正式な記録です。ソフトウェア開発者やベンダーは、既存のオープンソースや商用のソフトウェアコンポーネントを組み合わせて製品を作ることが多いです。SBOMは、製品に含まれるこれらの構成要素を列挙したものです。[3]

SaaS Security Posture Management （SSPM）。Slack、Salesforce、Microsoft 365などのクラウドベースのSaaSアプリケーションの自動継続監視を提供し、リスクの高い構成を最小限に抑え、構成ドリフトを防止し、セキュリティおよびITチームがコンプライアンスを確保できるよう支援します。

Secure Service Edge （SSE）。Web、クラウドサービス、プライベートアプリケーションへのアクセスを保護します。機能としては、アクセス制御、脅威防御、データセキュリティ、セキュリティ監視、ネットワークベースおよびAPIベースの統合によって実施される許容可能な利用コントロールが含まれます。SSEは、主にクラウドベースのサービスとして提供されますが、オンプレミスまたはエージェントベースのコンポーネントを含む場合もあります。

---

1 https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokerscasbs

2 https://csrc.nist.gov/glossary/term/software_as_a_service

3 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nationscybersecurity

17. 頭字語

AICPA - 米国公認会計士協会

API - アプリケーションインターフェース

CASB - クラウドアクセスセキュリティブローカー

CIA - 機密性、完全性、可用性

CCM - クラウドコントロールマトリックス

CSA CCM - クラウドセキュリティアライアンス クラウドコントロールマトリックス

CSA STAR - クラウドセキュリティアライアンス Security, Trust, Assurance, and Risk

CSC - クラウドサービスカスタマ

CSP - クラウドサービスプロバイダ

DLP - データ漏洩防止

FedRAMP - Federal Risk and Authorization Management Program

HIPAA - Health Insurance Portability and Accountability Act

HITRUST - Health Information Trust Alliance

IaaS - Infrastructure as a Service

IEC - 国際電気標準会議

ISMS - 情報セキュリティマネジメントシステム

ISO - 国際標準化機構

NIST - 国立標準技術研究所

MTD - Maximum Tolerable Downtime（最大許容停止時間）

OTP - ワンタイムパスワード

PaaS - Platform as a Service

PCI - Payment Card Industry

PII - 個人を特定できる情報

RFI - Request for Information

RPO - Recovery Time Objective 目標復旧時間

RTO - Recovery Point Objective 目標復旧ポイント

SaaS - Software as a Service

SASE - Secure Access Service Edge

SBOM - Software Bill of Materials

SIEM - Security Information and Event Management

SLA - サービスレベル合意書

SOC 1 - Service Organization Control 1

SOC 2 - Service Organization Control 2

SSE - Secure Service Edge

SSPM - SaaS Security Posture Management

TLS - Transport Layer Security

VM - 仮想マシン

ZTNA - ゼロトラストネットワークアーキテクチャ