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®

The permanent and official location for the SaaS Working Group is https://cloudsecurityalliance.org/research/working-groups/saas-governance/

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
2023 年 05 月 18 日	日本語版 1.1	全体の翻訳を改訂

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

日本語版 1.1 作成に際しての謝辞

日本語版 1.1 の作成は、CSA ジャパン会員の CASB WG 有志により行われました。（氏名あいうえお順・敬称略）

小野　貴博
根塚　昭憲
羽田　昌弘
吉田　豊満

目次

1. はじめに

組織は、2-3 社の IaaS プロバイダーを利用する傾向がある一方、数十から数百の SaaS プロバイダーを利用していることが多いという現実があります。それにもかかわらず、クラウドセキュリティの文脈では、ほとんどの場合、Infrastructure as a Service（IaaS）と Platform as a Service（PaaS）のセキュリティに焦点が当てられています。本書は、SaaS 環境における基礎的なガバナンス実践のためのベースラインセットを提示します。そして、評価、採用、使用、解約を含む、SaaS のライフサイクルの各段階におけるリスクを列挙し、考察します。

組織が SaaS によるアプリケーションやソリューションを今後も採用していくには、組織における従来のサイバーセキュリティの中でいくつかの領域を更新し、この新しい運用モデルを反映しなければなりません。

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しなければなりません。組織におけるセキュリティ運用の責任やタスクなどに影響があり、モバイルデバイスや従業員のリモートワークも関わってきます。情報は資産であり、外部のサービスプロバイダーが提供する SaaS では、情報の分類、ラベル付け、保管要件について考慮しなければなりません。責任共有モデルにおいて SaaS プロバイダーが多くの責任を負いますが、SaaS 利用者もデータガバナンスとアクセス制御に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ーにおいては、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、アクセスを認められるかを明確にすることに相当します。

組織には、暗号鍵の管理の他、脆弱性管理やバックアップ、データの保管といった運用に関わる重要な判断が残ります。組織は、SaaS プロバイダー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検討し、適宜、インシデント対応や事業継続の計画とプロセスを更新する必要があります。リモートワークの枠組みの中で、SaaS が事業継続における重要な機能を果たすことが多くなってきているため、これは、ますます重要になってきています。また、責任共有であっても、組織は、自組織のステークホルダーや評判を守り、潜在的な法的影響を回避するため、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、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に変化をもたらし、プロバイダーと利用者の間に責任の共有を導入します。この変化に応じた調整を怠ると、機微なデータの漏洩、収益の損失、顧客からの信頼の喪失、規制による影響など、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、以下を扱います。

- SaaS 環境内のデータを保護するため、SaaS ガバナンスベストプラクティスのベースラインセットを提供します。
- SaaS の採用や使用のライフサイクルに従って、リスクを列挙し、考察します。
- SaaS 利用者の視点から、軽減策の候補を提供します。

1.2 想定する読者

- SaaS 利用者
- SaaS プロバイダー
- SaaS セキュリティのソリューションプロバイダー
- クラウドセキュリティの専門家
- 法務部門
- サイバーセキュリティ担当役員
- IT 担当役員
- リスクの管理者
- IT 監査およびコンプライアンス部門
- サードパーティーリスクの管理者

2. 概要

Software as a Service（SaaS）の顧客や利用者は、SaaS サービスの利用によって生じる、情報セキュリティリスクを評価し、軽減するべきです。この文書では、NIST 800-145 の文脈を借用し、SaaS を「クラウドインフラ上で動作するプロバイダーのアプリケーションを使うことによって、利用者に提供される機能」と定義します。この文脈では、特定の設定を除いて、利用者が、クラウドインフラ、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管理または制御を行うことはありません。

クラウド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。組織における SaaS サービスの利用は増加しており、時には（Shadow IT として）組織内のさまざまな部門が利用し、重要なビジネスプロセスや機能に組み込んだり、しばしば機微なデータを SaaS 環境に保管したりしている現実にもかかわらずです。

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）のガバナンスと似た部分もありますが、SaaS の導入と管理の性質上、独自のアプローチが必要になります。SaaS に対して、セキュリティとガバナンスのデューデリジェンスを適切に行うには、SaaS アプリケーションの用途や機能を理解するといった抽象的なレベルから始まり、どのような種類のデータをシステムに保存し、誰にアクセスを認めるかといった詳細にまで踏み込まなければなりません。

SaaS アプリケーション利用の適切なガバナンスに固有の複雑さに加え、無数の SaaS アプリケーションが導入される可能性を考えると、組織はまず、組織のセキュリティ、ビジネス、および規制の要件にふさわしいフレームワーク（NIST Cybersecurity Framework など）を探すべきです。このフレームワークを使って、セキュリティアーキテクチャーを構成する、人、プロセス、技術の方向性を定めます。

NIST Cybersecurity Framework などの広く採用されているセキュリティフレームワークを、本書のベストプラクティスや推奨事項と組み合わせることによって、組織は、SaaS のガバナンスとセキュリティのプロセスを確立し、SaaS の利用にともな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 セキュリティに必要な 3 つの要素である、プロセス、プラットフォーム、アプリケーションを定義します。SaaS のための統合セキュリティは、統率が取れた戦略のもと、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結びつけることによって実現できます。

プロセスセキュリティは、手続きの完全性を保護し、プロセスの入力と出力が容易に損なわれないようにします。ポリシーや手順を含めた管理的な側面を持ち、組織のプロセスに一貫性を確保します。

プラットフォームセキュリティは、SaaS サービスの基礎的な依存関係にあたる、プラットフォームのセキュリティ強度を扱い、

SaaS のインフラ、オペレーティングシステム、そして、それらの潜在的なサプライヤーを含みます。

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身のセキュリティを扱います。SaaS アプリケーションは、悪用可能な脆弱性が存在せず、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従って、強固な設定を実装して初めて、安全性を維持することができます。

SaaS モデルでは、限られた制御と可視性が、プロセスセキュリティとアプリケーションセキュリティの構成要素の範囲に制限されます。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の構成要素や、それを支えるサプライチェーンを制御することができません。このような現実のため、SaaS 利用者は、組織内で堅実なプロセスセキュリティを確立し、アプリケーションレベルのセキュリティ管理策を確実に実装することが必要になります。

業界固有のセキュリティ管理策は、一般的に、プライバシー、規制、または財務のコンプライアンスを満たすために使います。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、業界に特化した内容で、SaaS の 3 つのセキュリティ領域にまたがります。

2.3 ライフサイクルの考察

適切なガバナンスが存在する場合、企業環境における SaaS アプリケーションの導入と利用は、評価、採用、使用という 3 つの主要なライフサイクルに従います。ここからは、これらのライフサイクルの一般的なパターンを説明します。

ただし、多くの組織では、SaaS アプリケーションの導入が自然に拡大し、SaaS アプリケーションの監視への対応が遅れている可能性が高いことに注意する必要があります。SaaS を幅広く採用した後に、SaaS のセキュリティとガバナンスのプログラムを導入する組織では、使用のライフサイクルが最も関連するでしょう。

2.3.1 評価のライフサイクル

評価のライフサイクルは、調達の前に行われ、SaaS アプリケーションが解決する可能性があるビジネスの要求事項の特定から始まります。多くの組織で、このライフサイクルは事業部門で行われ、組織全体の調達部門が関与する場合もあれば、しない場合もあります。評価のライフサイクルは、通常、4 つのステップで構成されます。

- 検討中のユースケースにおいて、既にユーザーが使っているサービスの把握
- マーケットの調査
- パイロットとしての試行
- 購入の判断

組織による購入が決定された場合、SaaS アプリケーションの展開が始まり、次に説明する、採用のライフサイクルが始まります。関連するセキュリティやコンプライアンス部門の代表者が、評価のライフサイクルから参加することが理想的です。一方、この後の採用のライフサイクルでは、そのような代表者の関与が不可欠です。組織が SaaS の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「チェックポイント」は、SaaS ライフサイクルにセキュリティチームを統合する重要なタイミングになります。

2.3.2 採用のライフサイクル

SaaS の採用ライフサイクルは、ほとんどの組織で同様です。このライフサイクルは、（パイロットプログラムを拡張する場合もありますが）対象の SaaS アプリケーションを最初に調達した時点から始まり、本格的な展開と利用の拡大を経て、将来的な解約と廃止までを含みます。

採用のライフサイクルの長さは、さまざまです。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、実際には、安定した状態に至ることもあります。しかし、採用のライフサイクルは、通常、4 つのステップで構成されます。

- **評価**：このフェーズでは、クラウド利用者が、利用を目的として SaaS アプリケーションの候補を評価します。一般的に、特徴、機能、ビジネスの要求事項への適合性を調査するため、パイロットや概念実証を実施します。
- **採用**：このフェーズでは、パイロットや概念実証を終えて、クラウド利用者が SaaS サービスを正式に採用します。このフェーズで、より機微なデータを SaaS アプリケーションに保管したり、追加のビジネス部門にアプリケーションを展開したりすることがあります。
- **日常的な使用と展開**：このフェーズは、継続のフェーズとも言えます。この時点で、クラウド利用者は、日常的に、この SaaS アプリケーションをさまざまなビジネス用途に使っており、また、その使用の標準的な運用手順が整備されています。
- **解約**：このフェーズは、クラウド利用者が、この SaaS サービスをこれ以上使わないと判断する時点を指します。コストやセキュリティ、あるいはビジネスの要求事項に合わなくなったためなど、さまざまな理由があります。クラウド利用者は、SaaS アプリケーションの利用を停止し始め、機微なデータやアカウントなどの取り扱いを減らします。

2.3.3 使用のライフサイクル

SaaS の使用ライフサイクルは、最小権限や Identity and Access Management など、日々の運用リスクやセキュリティ課題に対する保護を助けます。

SaaS の使用ライフサイクルは、4 つのステップで構成されます。

- **適格性**：この人や Non-person entity は、このサービスのユーザーになるべきですか。
- **プロビジョニング**：この人をサービスに追加するには、何の実施が必要ですか。この人は、どの権限が適切ですか。
- **監視**：この人は、組織が期待する使用方法に従って、文書化された範囲内でサービスを使っていますか。
- **デプロビジョニング**：この人を、どのようにサービスから削除しますか。

SaaS の使用ライフサイクルは、組織が、Cloud Service Provider（CSP）や SaaS サービスをどのように扱うかを明確にします。

SaaS の使用ライフサイクルの全体を理解して、監視することが重要です。ユーザーの登録など、ライフサイクルの 1 ステージに集中して、最適化してしまうことが非常に多いですが、そのようにしても、組織が望む結果を、簡単に、素早く得られることはありません。

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ーを構築するべきです。強固なセキュリティアーキテクチャーは、SaaS アプリケーションの展開と維持を導くためのセキュリティポリシーを備えるべきです。

3.1 情報セキュリティのためのポリシー

ポリシーは、SaaS サービスの評価、採用、使用、解約を統制するべきです。前章の一般的な SaaS ライフサイクルを参照し、ライフサイクルの各フェーズに対して、組織が包括的なポリシーと評価のための管理策を用意していることを確認します。

3.1.1 評価

あらゆる決定は、エンタープライズアーキテクチャーの要件とプロセスによって導かれるべきです。その環境の総合的なエンタープライズアーキテクチャー（製品、サービス、ツールの評価、およびそれらが解決する要求事項）を整備するべきです。これにより、製品、サービス、ツールの不要な重複を防ぎます。

既存のエンタープライズアーキテクチャーでは、対応できない要求事項が見つかってから、製品、サービス、ツールの評価を始めます。

通常、SaaS サービスの初期評価は、ビジネス、法務、セキュリティのステークホルダーが、この取引に関わるリスクを把握しながら進めます。重要な問いは、「自組織のリスクプロファイルやエンタープライズアーキテクチャーと調和するか」です。

3.1.1.1 許容リスクの決定

SaaS サービスを評価する最初のステップは、利用者が自組織のリスク選好に合わせて、どのようなリスクを想定するかを決めることです。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置かれることがあり、またアプリケーションレベルでも、専有もしくは共有リソース（シングルインスタンス、マルチテナント）で提供されます。クラウドのあらゆる製品、サービス、ツールと同様に、責任共有モデルを理解するべきです。

ISO/IEC 27001 に従って、リスクマネジメントのアプローチを情報セキュリティの管理に使うべきです。まず、SaaS 利用者は、SaaS サービスの利用にともなう、組織にとって許容可能なリスクを定め、評価段階のベースラインを用意するべきです。リスクの管理には、国際的なリスクマネジメントの標準である ISO 31000 など、さまざまな手法を使うことができます。

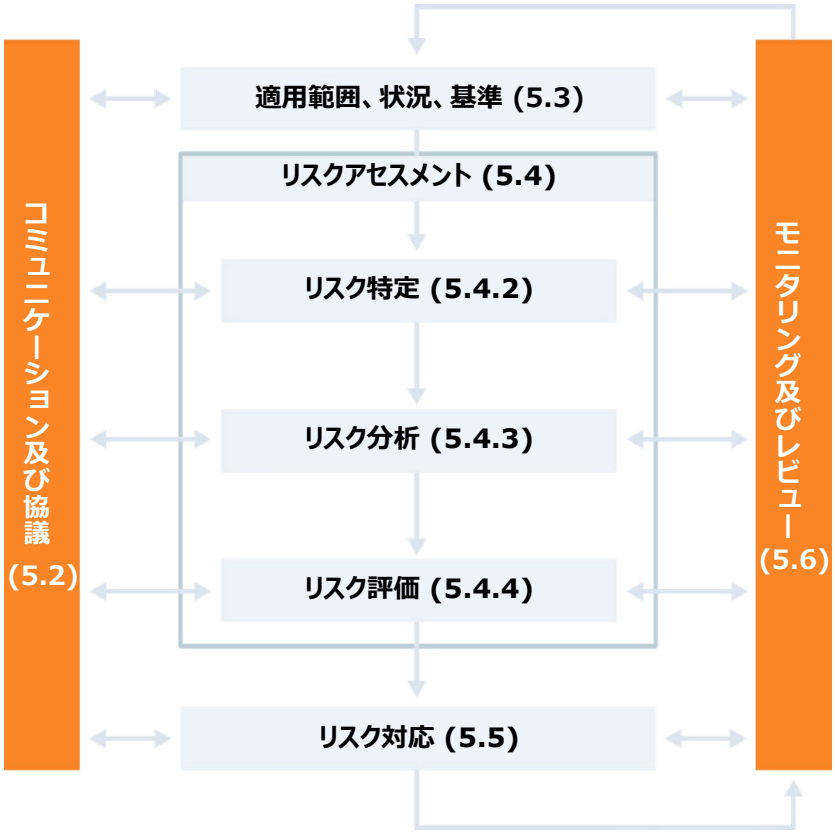

図 1. ISO のリスクマネジメントプロセス（Clause 5: プロセス）

組織のリスクプロファイルを理解することにより、SaaS 利用者は、評価中の SaaS サービスが組織のリスクプロファイルと調和する可能性があるかを判断できます。

SaaS サービスのリスクプロファイルを決めるには、以下を考慮しながら、SaaS サービスの利用コンテキストを把握する方法があります。

- データ
  - どのようなデータを、プロセスの中で保管し、SaaS アプリケーションに開示しますか。
  - SaaS アプリケーションに保存したデータの機密性や完全性が損なわれた場合、どのような直接コスト（影響を受けた個人への通知、株価下落による株主への影響、競合への大量の顧客流出、利益の損失）、間接コスト（評判の毀損と将来の売上減少、サイバー保険の費用増加、主要スタッフの解雇）、および隠れたコスト（対応のためのスタッフの配置転換、侵害箇所のセキュリティ強化）が、ビジネスに対して発生しますか。
- プロセス
  - このサービスは、主要なビジネスプロセスや、重要なビジネスプロセスに影響しますか。
  - この SaaS サービスを利用する場合、組織のどのポリシーやプロセスを見直す必要がありますか。
- 要件
  - どのようなビジネス要件、法律、および規制が、このサービスに関連しますか。

この段階で、SaaS 利用者のリスクプロファイルに与える影響という視点から、以下の項目を評価するべきです。

- 対象の SaaS プロバイダー
- 対象の SaaS サービス
- 対象の SaaS プロバイダーのサプライヤー
- 対象の SaaS サービスの用途
- SaaS 利用者が、対象の SaaS プロバイダーに対して継続的な監視と態勢管理を行い、リスクを軽減する能力

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 CIA による分類です。

- 機密性（Confidentiality）
- 完全性（Integrity）
- 情報の可用性（Availability）

CIA では、組織の要件に従って、アプリケーションやデータベースのリスクをスコア化します。

リスクの影響範囲を明確にしてから、SaaS アプリケーションに起因するリスクの計算を始めます。

リスクの計算方法は多様であり、リスクプロファイリングの枠組みの構築方法は、組織の要求事項や業界に依存します。

SaaS 利用者は、CSP に作業を移転しても、CSP に**説明責任をアウトソースすることができない**ことに留意する必要があります。SaaS 利用者は、SaaS サービスの採用にともなうリスクを受け入れる責任が、リスクの所有者にあることを常に念頭に置かなければなりません。CSP と利用者の間に責任の共有があり、サービスレベル合意書などの合意が存在しますが、最終的に、リスクを所有するのは利用者です。

3.1.1.2 セキュリティとプライバシーの要件

ベースラインとなるリスクレベルを確立すると、多くのクラウドサービス利用者は、セキュリティとプライバシーのデューデリジェンスのプロセスに取り組みます。クラウドサービス利用者にとって、評価用アンケートや Request for Information（RFI）を送付して、クラウドプロバイダーに回答を求めることが一般的です。

これらのアンケートでは、利用者が期待するセキュリティ管理策が CSP 内部に実装されているかを確認し、通常、セキュリティやプライバシーに関する規制要件に対応します。

CSA STAR Consensus Assessment Initiative Questionnaire などの自己評価のスキームや、第三者評価（SOC 2 や FedRAMP など）は、SaaS プロバイダーのセキュリティ関連の能力や既存の運用を、CSP が見込み顧客に伝えるために役立ちます。

このような自己評価や第三者の報告書は、クラウドプロバイダーによる個人情報の利用や提供、および個人情報をどこで処理するかについても質問します。これらの項目は、クラウドプロバイダーが個人情報を自社の目的のために使うのか、もしくは、（例えば、サードパーティーの広告主への開示など）第三者に提供するのかも確認します。

データ主権の要件が存在する場合があるため、データの所在にも注意が必要です。

以下は、第三者評価の主要なカテゴリーです。

- 認証と標準
- データ保護
- アクセス制御
- 監査への対応
- 災害対策と事業継続
- 法律とプライバシー
- 脆弱性と潜在的な脅威

3.1.1.3 要件の伝達

利用者は、これらのアンケートや報告書の回答を使って、リスクアセスメントをさらに精緻化し、クラウドとの取引の契約段階に活かすことができます。リスクアセスメントとデューデリジェンスのプロセスを補強するため、またサプライヤー管理の一部として、多くのクラウド利用者は、データセキュリティとプライバシーの標準的な別紙や条項を作成し、クラウドとの契約に反映しています。

これらの別紙や条項の目的は多岐にわたり、重大な結果につながる可能性があります。目的のひとつは、特定の地域内にデータを保持するなど、規制に対応することです。他にも、クラウドベンダーに合理的なセキュリティ標準を守らせる仕組みを作ることがあります。これらの別紙や条項は、インシデント対応時の義務を定め、クラウドプロバイダーに起因するデータ侵害やプライバシー違反による損失のリスクを移転する場合もあります。また、データ侵害などの問題に対して、指定した時間内に、指定した方法で対応することを求めたり、監査の権利や、定期的な監視や管理を行う権利を含めたりする場合もあります。

さらに、CSP と利用者の間の契約を執行または統治する、関連する法的管轄や、規制の枠組みを理解することが不可欠です。例えば、従業員や顧客の個人情報を保存して、処理するための SaaS プラットフォームを探しており、かつ、GDPR が適用される場合、CSP が、EU や EEA の地域、もしくは適切な保護を提供する国にデータを保存しているかを確認する必要があります。そうでない場合、データが保存される国に適用される法的枠組みを理解し、CSP が適切な保護を備えていることを確認し、欧州連合司法裁判所（the Court of Justice of the European Union）の Schrems II 判決に従ってデータ保護のための補完的な技術的対策を実施する必要があります。

全体的な目的は、契約面で調和がとれた関係をクラウドプロバイダーと構築し、利用者のリスクをできるだけ低減することです。

ベンダー管理プログラムにおける契約プロセスは、利用者が、クラウドプロバイダーとの交渉の中で、特定条件下における「代替策」をあらかじめ規定することにより、さらに改善されることがあります。これには、（ベンダーロックインを防ぐため）契約終了を判断した場合における、データなどの移行方法を含むことがあります。このような条件交渉に、利用者の法務チームとセキュリティチームが揃って関与することは、珍しくありません。

3.1.1.4 組織内の管理策

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ーを構築するべきです。SaaS 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を念頭に置くべきです。すなわち、SaaS プロバイダーではなく、SaaS 利用者が、設計された制限内における、SaaS プラットフォームの安全な構成、管理、および利用に対して最終的な責任を負います。

脅威モデリングと脅威プロファイリングは、SaaS のセキュリティ戦略を策定するために重要です。Cloud Security Alliance は、「脅威モデリングのセキュリティ目標を明確にし、評価のスコープを設定し、システムを分解し、脅威を特定し、設計上の脆弱性を特定し、軽減策と管理策を策定し、行動を促すコミュニケーションを行うための重要なガイドラインを提供する」ために、Cloud Threat Modeling を発行しました。

クラウドであるかに関わらず、他の技術と同様に、SaaS プラットフォーム利用のための効果的なリスクマネジメントとセキュリティ管理策には、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合わせて、SaaS 利用者が多方面からのセキュリティ戦略を導入する必要があります。この戦略には、次のような要素を含みます。

- SaaS プラットフォームに適用可能な、クラウドサービス利用者に関わるセキュリティ管理策と構成（SSO、MFA、ロールの割り当て、チームやグループの分離、ログのエクスポートやセキュリティ監視ソリューションとの統合、IP アドレスの制限など）を把握し、採用します。
- SaaS の利用状況とその妥当性を定期的にレビューします。
- SaaS アプリケーションやプラットフォームから管理または展開している、ビジネスロジックやプロセスを対象にペネトレーションテストを実施します。
- SaaS アプリケーションの構成を、組織に固有の承認済の構成や期待される構成と比較して、セキュリティ態勢を継続的に監視します。
- SaaS アプリケーションが生成する監査ログ、イベントログ、その他の変更やアクティビティのログを継続的に監視します。理想的には、他の SaaS や SaaS 以外のアプリケーションと、これらのログを相関させることができる環境で監視します。
- SaaS アプリケーション内の重要なデータやプロセスへのアクセスを継続的に監視します。

3.1.1.5 サービス条項

信頼できるインシデント対応や、セキュリティやフォレンジックの評価を行う権利の交渉に失敗するとリスクが生じます。

SaaS プロバイダーが利用者の情報に影響を与える侵害を受けても、その侵害を通知し、修復を行い、協力することが契約上の義務になっていない場合、その SaaS 利用者は、自組織の法的リスクを軽減し、規制上の義務を遵守できない可能性があります。各地域の法律や通知義務はさまざまです。そのため、調達や契約の段階で、サイバー領域に精通した法律の専門家が関わることが重要です。

検討すべき契約上の管理策：

- サービスレベルの管理
  - サービスプロバイダーの SLA と、組織の SLA 要件の比較（リソースやサポートの側面を含む）
  - 事業継続性に関する保証：RPO および RTO と、組織の MTD[1]の比較
  - インシデントへの対応とエスカレーション
- バックアップの可用性
- 法的な懸念事項
  - 法律および規制に関する要件

[1] 訳注：Maximum Tolerable Downtime

    - CSP と SaaS サービスに関する裁判管轄と法的な要件
    - 損害補償、裁判管轄の移転、M&A
- セキュリティ、プライバシー、コンプライアンスに関わる変更や事象の通知
- 解約の権利と手続き
    - データの可搬性（他プラットフォームに移行する場合、データをエクスポートする手段の検討が必要）
    - データの削除、削除までにかかる時間、削除完了の書面による通知
    - アウトソーシング契約を終了する場合の出口戦略

3.1.1.6 データへの影響

クラウドコンピューティングへの移行にともなう重要なリスクには、クラウドに転送したデータ、および、クラウドにアウトソースしたネットワークの可用性に対して、絶対的な制御を失うことがあります。

例えば、従来の IT 環境では、適用される規制や標準に準拠するため、自組織のシステムを評価して、必要な対応を行うことができます。これには、組織やその顧客の所在地にもとづく、データの所在に関する要件を含むことがあります。

多くの SaaS プロバイダーは、複数の裁判管轄にまたがる IaaS プロバイダーを使うため、このような要件を考慮せずに SaaS サービスを使うと、コンプライアンスに対するリスクが増加する可能性があります。

SaaS 利用者は、以下の質問に答えられるべきです。

- SaaS プロバイダーは、どの裁判管轄で事業を営んでいますか。
- どのような規制要件が適用されますか。
- SaaS サービスに、どのようなデータを転送しますか。
- SaaS サービスは、どのようなデータにアクセスできますか。
- 自組織のデータに関して、SaaS サービスにどのような依存関係が生じますか。
- CSP がどのような法的義務を負っていますか。例えば、決済事業者は、マネーロンダリング対策の法的義務を遵守するため、特定のデータを保持する必要があります。
- 仮に、政府や軍の組織がデータへのアクセスを要求した場合、SaaS プロバイダーはどのように対応しますか。

例えば、機微ではないデータのみを SaaS アプリケーションに保存する場合は、機微なデータ（社会保障番号や金融口座データなど）を扱う場合と比べて、サプライヤーに対する調査が軽微で済む場合があります。

管理策：

- データの価値に合わせた機密性要件
- データ分類に関する要件（HIPAA、PCI など）
- データやメタデータの統制（所有権、処理方法、ライセンス供与）
- データの所在と主権
- 可用性要件とデータの移動性

3.1.1.7 プライバシー

SaaS プロバイダーを利用する場合、そのプロバイダー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、利用者が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対して、どのような用途（機械学習や匿名データセットの評価など）がプロバイダーに許可されているかを理解するべきです。このような用途がある場合、SaaS 利用者の規制や監査の要件に準拠するべきです。

変化を続ける規制の情勢は、プライバシー関連のコンプライアンスやデータ所在違反のリスクを高めており、一部の利用者や特定の種類のデータにとって、SaaS アプリケーションの採用を複雑にしています。ヨーロッパ市民のデータを預かるアメリカの SaaS プロバイダーに対する懸念は、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 サービスの役割の明確化
  - コントローラー（顧客や従業員の個人情報を管理）
  - プロセッサー（コントローラーが提供する個人情報を処理）
- プライバシーポリシー：サービス内にあるデータに対する SaaS プロバイダーの権利
- 違反時の義務と責任
- 個人情報の管理台帳と可視性
- 同意の管理

3.1.1.8 詳細リスクアセスメントのためのステップ

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. Fluid risk-to-asset tracking[2]の実施

[2] 訳注：リスクと資産を紐づけるためのアプローチのひとつ

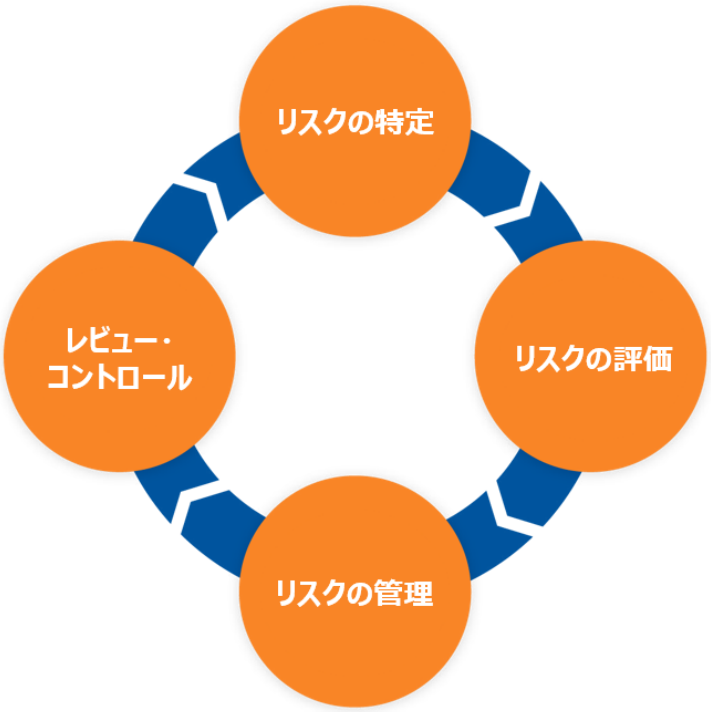

図 2. リスクアセスメントのサイクル

3.1.1.9 リスクの特定

ビジネスの目的を妨げる可能性があるリスクの領域を以下に示します。

- データ、財務情報、知的財産、競争上の優位性の喪失
- 規制や法による義務
- 企業の評判
- 脅威、脆弱性、攻撃
- インシデント管理
- 技術的な複雑性
    - 従業員の専門性
    - 財務的な責任
- サードパーティーサプライヤー
- 第三者監査、SOC 2 報告書、STAR Registry など
- 人による過失

3.1.1.10 リスクの評価

- 定性的および定量的なリスクアセスメント
- Governance Risk Compliance（GRC）
- リスク許容度もしくはリスク選好

3.1.1.11 リスクの管理

- リスク許容度に合わせて、物理的、技術的、管理的な対策を実装
- 第三者へのリスクの移転
- リスクの受容

3.1.1.12 管理策のレビュー

- 内部監査および外部監査
- リスク分析

（訳注：ここから、管理策のレビューではなく、リスクアセスメントについての説明が始まります）

リスクを特定するには、SaaS サービスと CSP に対する詳細リスクアセスメントが必須です。

リスクアセスメントは、組織の資産を CSP のクラウドに置く前に実施するべきです。リスクアセスメントに必要な詳細さは、環境によって異なります。例えば、限定したユースケース（サンドボックス、ソフトウェア開発、CSP の機能や管理策のテストなど）で CSP を使い始める場合があります。このシナリオでは、「最小限のリスクアセスメント」で十分かもしれません。CSP のツールや機能が利用者のビジネスの目的を満たす場合、より詳細なリスクアセスメントを行ってから、アプリケーションを本番移行するべきです。

SaaS のリスクアセスメントでは、次の 3 つの領域を注意深く調査するべきです。a）SaaS プロバイダー、b）SaaS プロバイダーによる管理運用、c）SaaS アプリケーションの技術的なセキュリティ検討です。下表では、検討すべき領域を列挙します。

プロバイダー	運用	アプリケーション
CSP は、どのような認証を保持していますか。	リージョン間やゾーン間のデータ転送を論理的に制限するため、CSP は、どのような管理策を採用していますか。	（IAM、RBAC、アカウント管理ツールなどを使って）アプリケーションアカウントや特権アカウントを、一元管理していますか。
CSP は、第三者による評価や監査を受けていますか。CSP は、SOC 2 報告書（または同等の報告書）を提供できますか。	（アプリケーション、データ、仮想マシンなどのため）CSP は、どのようなバックアップやリストアのサービスを提供していますか。	（パスワード、証明書、データの安全な転送のために）安全な通信経路を用意していますか。
利用者のデータは、CSP の施設内に保存されていますか。それとも、CSP は、（データセンター機能を）サードパーティーのサプライヤーと契約していますか。	CSP は、どのようなインシデント管理プロセスを用意していますか。どのようにインシデントを分類していますか。	安全な認証のため、SSO、SAML、MFA を使っていますか。

プロバイダー	運用	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、利用者にどのレベルのサポートを提供していますか。	仮想マシンイメージ、サーバー、データベースに、定期的にパッチを適用していますか。CSP は、どのようなアンチウイルスの管理プロセスを採用していますか。	アプリケーションやストレージのアカウントは、一般に公開されていますか。
CSP は、どのような SLA や OLA を用意していますか。	どのように暗号鍵の管理や保管などを行っていますか。誰が暗号鍵にアクセスできますか。	アプリケーションやソフトウェアは、クラウド用にライセンス供与されていますか。
CSP は、この SaaS を支える、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。提供している場合、CSP は、バックグラウンドチェックや NDA を採用していますか。	どのようなログ出力、SIEM イベント、脅威検知ツールを、利用者に提供していますか。	ソフトウェアやデータは、規制やプライバシーの要件の対象になりますか。
CSP は、どのような標準や規制要件に準拠できますか。 CSP のベースライン管理策は、どの標準 （ ISO 、NIST 、CIS 、PCI 、HIPAA、GDPR など）に対応付けられていますか。	CSP は、どのような IDS や IPS のツールを提供していますか。	どのようなソフトウェア開発プロセスやツール （ DevSecOps 、GitHub 、SDLC など）が、アプリケーションの開発やメンテナンスに必要ですか。CSP は、上記作業をサポートするため、どのようなツールやアプリケーションを使いっていますか。
CSP を支えるアーキテクチャーは、業界のベストプラクティスや標準を使って設計および開発されていますか。	CSP は、セキュリティ強化した仮想マシンイメージを提供していますか。どのように、これらのイメージを管理および適用していますか。	アプリケーションをサポートするため、どのような API が必要ですか。CSP は、どのような支援を提供できますか。
CSP は、自動化ツールや、クラウドリソースを構築するスクリプト（仮想マシン、IaC、自動修復など）を利用または提供していますか。	CSP は、データの不正流出を防止する管理策を提供していますか。	（必要な場合）CSP は、アプリケーションの脆弱性診断やペネトレーションテストをサポートしますか。

誤解のないように説明すると、上記のリスク評価は、SaaS プロバイダー、それを支えるアーキテクチャー、およびアプリケーションの実装のセキュリティに限定しています。SaaS 利用者が行う、SaaS アプリケーションの実装や利用に対する、継続的なセキュリティ監視やリスクの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には、さまざまなレンズを通して SaaS を理解しなければなりません。そのようにして初めて、SaaS のリスクを適切に特定し、評価し、軽減したという一定の保証を得ることができます。リスクアセスメントは、「1 回で完結する」作業と捉えるべきではありません。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べきです。

SaaS 利用者は、自組織に必要なソリューションの要件を把握し、それらの要件が SaaS プロバイダーに理解され、実現できることを確認する必要があります。SaaS プロバイダーが、あなたのアプリケーションや業界に必要な、特定のサービスや管理策を提供していない場合を考えてください。このような場合、そのギャップを軽減するか、もしくは、そのプロバイダーを使わないことを選択するかは、SaaS 利用者の責任です。

3.1.1.13 クラウドプロバイダー評価のベストプラクティス

- サードパーティーの技術サービスを自組織の資産として扱います。
- サードパーティーを評価するための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入力にもとづく、サードパーティーの評価を開発します。
- ビジネスオーナーを関与させます。
- リスクの高いベンダーを定期的にレビューします。
- 認可済のベンダーやアプリケーション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、認可済のベンダーやアプリケーションの使用を求めます。
- 事前承認したベンダーを組織全体で使えないか検討します。
- コンプライアンスに準拠したサプライヤーの使用を推奨もしくは強制します。

3.1.1.14 ポリシーと手続きの策定

SaaS アプリケーションを安全に導入し、活用するためには、SaaS 利用者が組織内のポリシーと手続きを策定し、SaaS アプリケーションの実装と利用を継続的に評価し、監視することが重要です。この章で前述した定期的なリスクのレビューと評価は、SaaS プロバイダーの技術、運用、認証を対象としています。SaaS 利用者が、SaaS アプリケーションの構成や実際の利用を監視し、評価する手段を導入することは、少なくとも同じくらい重要です。

このようなポリシーには、少なくとも、以下を含むべきです。

- アカウント管理の手続き
- 一元化したアイデンティティ管理の手続き
- データやシステムへのアクセス要件（重要なアクセスを付与する際の承認、および、そのようなアカウントに対する追加の認証要求など）
- サービスの不正利用を防ぐための利用規定
- ビジネスプロセスと統合したユーザーのライフサイクル
- データの分類とラベル付け
- 既存のサービスレベル管理、インシデント管理、脆弱性管理のプロセスへの統合
- 既存のガバナンスメカニズムへの統合、および必要に応じた作成および改修（変更管理など）

他のセキュリティプログラムと同様、SaaS アプリケーションの構成や、データの分類、データアクセスの監視を 1 回限りの作業ではありません。SaaS は、他のクラウド技術よりも変化が激しく、すぐに構成を変更することができます。SaaS 利用者の管理者は、1 回の不注意なコマンドやボタンのクリックで、SaaS アプリケーションのセキュリティ態勢を大幅に変更することができるため、継続的な監視プログラムの必要性がさらに強調されます。

3.1.1.15 構成とセキュリティ態勢の管理

重要な SaaS アプリケーションは、システムに保存している機微なデータや、侵害時のビジネス中断の可能性などの指標によって定義され、このようなアプリケーションは、継続的に監視しなければなりません。このような監視機能は、できれば自動化して頻繁に実行し、また大きな変更後にその場で実行できるべきです。理想的には、サンドボックスや本番前の環境に対しても実行でき、本番の SaaS 環境に反映する前に、構成変更を検証することができるべきです。

少なくとも、重要な SaaS アプリケーションのために、SaaS 利用者の態勢管理プログラムは、以下を考慮するべきです。

- 特に以下の設定に関連するシステム設定の構成ベースライン
  - アイデンティティ
  - MFA、SSO、地理や IP アドレスによる制限を含む、認証とシステムへのアクセス
  - パスワードポリシー
  - セッション制御
  - 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と BYOK 機能
- インストールされた承認済のサードパーティープラグイン、インテグレーション、OAuth などのクラウド間接続
- ロール、プロファイル、グループ、チームなど、追加のアクセスや機能を付与できる SaaS アプリケーションのエンティティへのユーザーの割り当て
- アクセスを付与する要素の構成と、この要素がユーザーに与える実効的なアクセス
- 機微もしくは特権的な行動を示唆する管理者の行動や認可のログ
- 主要な SaaS アプリケーションや環境を横断した行動の相関
- 主要な種類のデータやレコードへのユーザーアクセスと、読取アクセス（機密性）か書込アクセス（完全性）かの判断
- オフボードの手続き

この章の構成管理は、「構成の制御（Configuration control）」を指します。NIST 800-53, CM-2 では、次のように述べています。「ベースライン構成は、将来のビルド、リリース、またはシステム変更の基礎を提供し、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、ネットワークトポロジー、およびシステムアーキテクチャー内のコンポーネントの論理配置などを含みます。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ります。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ーを反映します。」

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、アプリケーションおよびサービスを迅速に開発しやすくなることです。現在の主要な SaaS アプリケーションでは、ローコードもしくはノーコードのアプリケーションの作成と展開を含むことが多く、これらのアプリケーションが重要なビジネスプロセスを制御します。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展開され、変更されます。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っており、このような権限の誤った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です。

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 利用者や SaaS プロバイダーが開発していない）サードパーティーのアプリケーションを使っ

て、SaaS プラットフォームを迅速に拡張できます。これは強力な反面、ベンダーのリスクア評価や調達プログラムから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、セキュリティ部門にとっては、承認された SaaS プラットフォームに対して、サードパーティーアプリケーションが未承認のまま接続されることを検知するため、監視と警告の機能を備えることが重要です。

ある SaaS プラットフォームを、他のいくつかの SaaS プラットフォームと接続する SaaS エコシステムでは、統合する前に、権限や統合の内容を正しく理解することが不可欠です。統合について十分な情報が得られない場合、重要度の低い環境やサンドボックスで統合を試してみる必要があるかもしれません。

例えば、Marketing Automation Platform（MAP）と Customer Relationship Management（CRM）プラットフォームを統合し、MAP のデータを CRM に取り込む場合を考えてみましょう。このシナリオでは、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、あるいは、CRM から MAP でしょうか。この場合、MAP から CRM です。

次に、この CRM が、マーケットプレイスで事前に検証され、統合されているかを確認する必要があります。通常、マーケットプレイスが提供する統合は、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ます。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します。

最後に、どのように最小権限を確保し、データ最小化の原則に従うかを分析する必要があります。

また、接続解除の方法を理解することも重要です。

別の例として、ユーザーが自分の Google アカウントをサードパーティーアプリケーションと統合する場合を考えてみましょう。ユーザーは、主に、どのような権限とスコープをサードパーティーアプリケーションに提供して、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確認する必要があります。その後、組織のリスク選好度にもとづいて判断します。このとき、ユーザーはセキュリティの専門家のサポートが必要でしょう。また、サードパーティーのアクセスを取り消す方法を知る必要があるかもしれません。

セキュリティ態勢管理のポリシーやルールを策定する際、SaaS 利用者は、業界のベストプラクティス（CIS Benchmark for Microsoft 365 など）を活用したり、リサーチにもとづいてベースラインのセキュリティポリシーを提供する SaaS Security Posture Management ベンダーと協力したり、自組織向けのベストプラクティスや要件を組織内で用意したりすることができます。多くの場合、これらのオプションを組み合わせて、より包括的なポリシーを策定します。

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態勢の監視と同様に、SaaS アプリケーションに保存した機微なデータへのアクセスを監視する必要があります。SaaS アプリケーションに固有の柔軟性と容易な設定により、ユーザーが持つデータへのアクセスはすぐに変わる可能性があります。したがって、他の SaaS のセキュリティ監視と同様に、データへのアクセスの監視も、1 回限りの作業ではなく、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やアクセス監視のソリューションの一部として、SaaS 利用者は、機微の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）データを分類するべきです。この分類は、外部システムで管

理しているか、SaaS プラットフォーム自身で管理しているかを問わず、データセキュリティポリシーを設計し、そのポリシーに対して現状を監視するために極めて重要です。

これ以外のデータセキュリティに関する考慮事項は、セキュリティ態勢監視の一部として監視できる可能性が高いですが、それでも明確に定義するべきです。考慮事項は、以下を含みます。

- データエクスポート機能やデータバックアップ機能の構成（および、それらへのユーザーアクセス）
- 資産、所有権、責任の管理台帳
- 社内および社外との共有に関する制限と、そのポリシーに合わせたシステム構成の監視
- 暗号化に関する管理策と要件、および意図通りに構成されているかを確認するためのシステム監視

SaaS アプリケーションに適用できる他の種類のセキュリティソリューションは、Data Loss Prevention（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したり、SaaS アプリケーションの組込機能として提供されたりします。DLP は、より高いレベルで情報保護を実現するために役立ち、特定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ます。最初にデータや文書を分類する必要があり、DLP ソリューションはこれらの分類を理解して、分類に応じた監視を行います（PII、PCI など）。

DLP は、主にキーワードや、フレーズ、メタデータにもとづいて動作します。DLP のロジックに一致すると、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、機微データの削除、調査やフォレンジックのためのデータ複製など、いくつかのアクションを実行することができます。SaaS プロバイダーは、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。非常に多くの SaaS システムを利用している場合、利用者は、調和がとれた管理のために SaaS プラットフォームと統合された DLP ソリューションを選択することがあります。

3.1.1.17 ユーザーの意識向上とトレーニング

- このサービスを安全に利用するためのベストプラクティスのガイドラインを策定します。
- データの分類とラベル付けを強制します。
- このサービスにおけるセキュリティインシデントと報告方法について、ユーザーの意識を向上させます。
- 可能な限りコーチングポリシーを追加します。（ユーザーにポップアップを表示して、カテゴリー内の認可済サービスにアクセスするよう求め、そうでない場合、他サービスを使用する正当な理由を記録させる、など）
- 率直な報告に対して報復を認めない雰囲気を醸成します。

3.1.1.18 内部脅威

- 退職する従業員が SaaS のデータを個人アカウントと共有し、組織のデータが流出する可能性があります。
- 組織内で、従業員が機微なデータを過剰に共有する可能性があります。（財務部門とエンジニアリング部門が互いの情報を利用できるかもしれません）
- 機微なデータを不適切なサードパーティーに共有する可能性があります。
- 職務が分離されていない可能性があります。
- 不適切なプラットフォームの構成によって、データが公開される可能性があります。（機微なデータを保存した S3 バケットを一般に公開するなど）
- 従業員がシステムのデータダンプを取得できる場合、その従業員の退職時に、データの漏洩や持ち出しにつなが

る可能性があります。

3.1.1.19 外部脅威

- サードパーティーの協力者が、組織のデータに永続的なアクセス権を持つ可能性があります。
- 委託先ベンダーが、組織のサードパーティーリスクアセスメントを経ていない再委託先ベンダーに、組織のデータを共有する可能性があります。
- 組織のデータを、個人アカウントで取り扱うサードパーティーの協力者のほとんどは、多要素認証を設定していない可能性があります。
- サードパーティベンダーやその委託先およびサプライヤーは、データ保護について規制当局から拘束されていない可能性があります。

3.1.2 使用

- 許容される使用
- アドミニストレーション
- ガバナンス

3.1.2.1 サービスやサプライヤーの定期レビュー

- サービス利用規約の変更の監視と、バージョンのアーカイブ
- 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 のサプライヤーを管理することは、難しい課題です。

3.1.2.2 アラート

- 不審なログインやデータアクセスを監視します。
- サービスの利用状況や不正利用を監視します。
- SLA 遵守のためのサービス属性を監視します。
- ログインやアクセスの以上を監視します。
- リスクがあり、組織全体に影響する設定変更を監視します。
- データへの異常なアクセスを監視します。

サービス利用規約が一晩で変更され、制御を失う可能性があります。そのため、自動化されたツールを使って、サービス属性を継続的に監視する必要があります。

必要に応じて、構成変更を監視し、アラートを通知します。

3.1.2.3 利用の可視化

- ログインやユーザーの場所を含む認証ログ
- アクセスログ
- 監査ログ
- アカウントのプロビジョンやでプロビジョンのログ

3.1.2.4 攻撃対象領域の継続評価と削減

- サービスの基本的な属性を監視し、健全性を確認します。
- 管理策をレビューし、攻撃ベクトルを減らします。
- 潜在的な組織内の障害ポイントを監視します。

3.1.2.5 構成管理

- 構成変更を監視し、必要に応じてアラートを通知します。

3.1.2.6 データ

- 機微なデータ、システム、フィールドへのアクセスを監視します。
- 管理的な操作を監視します。
- 監査を有効にします。
- バックアップの有効性を監視します。

データがバックアップされていることを確認します。より重要なことは、リストアを実行または要求し、取得したバックアップをテストすることです。

3.1.3 解約

SaaS 利用の解約には、調整と計画的な実行が必要です。

最も重要ですが見落としがちな SaaS サービスのリスクは、CSP が提示する契約にあります。

従来、組織は法務部門と協力して、サービスプロバイダーの契約条件が「ベンダーの都合」に寄り過ぎないように交渉し、サービスプロバイダーに金銭的な責任を課すことにより、サービスプロバイダーに起因する損失を軽減してきました。しかし、クラウドプロバイダーは、特にプライバシーやデータセキュリティに関して、一般的な補償、法的責任の制限、その他の条件などを提示することに積極的ではありません。

CSP がよく挙げる理由には、これらの追加された義務や責任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や、CSP は利用者がクラウドに何を保存しているかを把握できないため、利用者データの分離や安全確保に対して責任を負うことができないことです。しかし、CSP は利用者がこれらを達成する手段を提供しなければなりません。

クラウド契約内の不都合な条件は、クラウドサービスの利用者のリスクを大きくするかもしれません。

また、クラウドサービスの利用者は、利用者のデータの保存や処理を行う CSP の委託先を、契約で制限することを望むかもしれません。このような制限がない場合、利用者のデータが、実際には、プライマリ CSP から 2 段か 3 段離れた場所にあることに気付くかもしれません。

3.1.3.1 組織内のプロセス

- すべてのユーザーにサービスの終了を通知します。
- すべての API アクセスを無効にします。
- 代替手段やデータ抽出に関するガイドラインを用意します。
- 今後の利用や他サービスへの移行のために、データを抽出します。
- 保存場所と責任者を明確にします。
- 他システムとのすべての統合やデータフローを把握します。

3.1.3.2 データの保持

- バックアップ、および、残存するデータやメタデータ（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）の破棄
- データ分類の要件を満たすデータ保持期間
- 財務情報のエクスポートおよび削除
- 利用状況などのレポートのエクスポート

3.1.3.3 資産の回収

- データやメタデータ（監査ログ、アクセスログ、バックアップなど）のエクスポート
- データの所在に関する要件の遵守
- 許容できるデータフォーマット
- 提供までの時間、方法、利用可能な期間

3.1.3.4 サービスの周辺機能の廃止

- サービス個別の監視
- サービスのセキュリティ監視

3.1.3.5 サービスの管理

- サービスとのすべての統合の解除
- サービス廃止の確認
- 契約終了の確認

3.2 情報セキュリティポリシーの見直し

技術が頻繁に変化するため、ポリシーの定期的な見直しが必要です。最後のバージョン以降、追加の許容可能な管理策が必要になるかもしれません。この際、SaaS の運用が、組織が定める必要最低限の標準を満たす必要があります。

CASB のようなソリューションプロバイダーは、SaaS サービスの継続的な評価とスコアリングを行い、この動的なスコアにもとづいてアラートやアクセスポリシーを設定する機能を提供します。

4. 情報セキュリティの組織

4.1 組織内

4.1.1 情報セキュリティの役割と責任

多くの人が SaaS を責任のアウトソースと捉えていますが、クラウドサービスの利用者（Cloud Service Customer; CSC）とクラウドサービスプロバイダー（Cloud Service Provider; CSP）の間の役割と責任を明確に理解することが極めて重要です。CSC が、候補の CSP との契約前、デューケアやデューデリジェンスを行う際に、思い込みや誤解を避けることができます。また、CSP と CSC の責任の区別にも役立ちます。CSP が何に責任を負うかよりも、CSP が何に責任を負わないかを知ることの方が、より多くを伝えると言えます。

（責任共有モデルが説明するように）CSP と CSC の間の役割と責任の分担を十分に理解すると、CSC が制御できない管理の側面が多くあることが明らかになります。一般的に、ほとんどの SaaS の実装では、CSC がアプリケーションやデータへのアクセス付与に責任を負うと理解されています。一方、CSP がそれ以外のすべてに責任を負います（すなわち、SaaS 利用者は、自身の管理下にないため、仮想マシンの既知の脆弱性を軽減することができません）。このため、CSC は、セキュリティとメンテナンスに関するほとんどの活動を CSP に委ねることになります。

SaaS ソリューションの機能の中には、CSC が責任を負うものがあります。この場合、CSC はこの課題を受け入れ、時間をかけてリスクを理解し、適切な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）を許容す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、アプリケーションが TLS 1.3 のみを許容す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 の利用を求めることもできます。

このような背景のもと、SaaS 利用者は、管理的対策と技術的対策を組み合わせて、自身の資産やリソースを、SaaS プラットフォームへの依存によるセキュリティリスクや運用リスクから保護する必要があります。下表は、CSC が実装すべき管理策を示します。ただし、実際に必要な技術的対策は、CSP によって異なることに注意してください。

技術的対策	管理的対策
セキュリティ監査やログ出力のためのシステムアプリケーションアカウント	ユーザーやシステムの認証
特権アカウントのための多要素認証	ユーザーやシステムへの認可
システムによる特権アカウントの監視	すべての特権アカウントを対象に、毎年、アカウント所有者が必要性を証明
すべてのアカウントを対象とした Identity and Access Management（IAM）ツール	暗号鍵の所有権の確認
暗号鍵、電子証明書などの安全なリポジトリ	クラウドコンピューティングのすべてのリソースや資産の棚卸と追跡

技術的対策	管理的対策
安全な通信経路（HTTPS、SSH、TLS、SFTP など）	ネットワークおよび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や資産に対する単一のビュー（SIEM、ログ統合など）	• ユーザーの認可 • メトリクス • コンプライアンスレポート
脆弱性管理 パッチ管理 是正と修正	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、通知、管理について、CSP と CSC の間での調整
（以下を含む）リスクマネジメントの評価ツール： • 脆弱性スキャン • 脅威モデリング • ペネトレーションテスト	• リスクマネジメントの承認とレビュー • 主要なリスクの指標 • 関連するステークホルダーへの指摘事項の通知 • 知識の移転

注：CSC と CSP の共有責任の詳細は、CSA's Enterprise Architecture - CCM Shared Responsibility Model を参照してください。

4.1.2 職務分掌

職務分掌（Segregation of Duties）のセキュリティ原則を実施するために管理策を実装しなければなりません。簡単に言うと、職務分掌とは、重要な業務の遂行に 2 人以上の人物や組織の関与を保証することで、不正や共謀の防止を目的とします。

NIST 800-145 の「Cloud Computing」の定義によると、クラウドに必須の特徴として、「オンデマンドなセルフサービス」が挙げられています。「オンデマンドなセルフサービス」とは、「利用者が、利用者自身の判断で、サーバーの稼働時間やネットワークストレージなどの計算能力を、必要なときに、人とのやり取りを介さず、自動的に調達できる」ことを意味します。つまり、「オンデマンドなセルフサービス」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では、エンドユーザーに技術的な専門知識が十分になくても、迅速かつ容易にクラウドのリソースや資産を起動することができます。これは、職務分掌を非常に複雑にし、簡単に制御を失いかねないことを意味します。

ユーザーやアプリケーションが作成または起動するクラウドリソースには、（ユーザーアカウント、システムアカウント、アプリケーションアカウント、ロール、グループなど）さまざまな形態があります。利用者は、これらのリソースがアクセスできる（クラウド境界の内側および外側の）範囲や、これらの ID に関連付けられた権限を把握し、これらのアカウントが、特定タスクの実行のために最小限の権限のみを持つように、適切に対応するべきです。この対応に失敗すると、意図しないリソースに対して、アカウントがアクセスを持つ可能性があります。職務分掌の管理策がないと、機密情報やプライバシー情報の不正な開示、データの損失、完全性の喪失などのリスクがあります。

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担いますが、CSC は、それでも、クラウド内で起きるすべてに説明責任を負います。これは、CSC が、契約の締結時に、「利用規約」、提供されるサービス、および制限事項に同意しているためです。

CSC は、インシデントの発生時や、SLA（Service Level Agreement）や OLA（Operating Level Agreement）の変更時に、主要なステークホルダーが通知を受けるためのプロセスを文書化するべきです。CSC はこの文書を CSP と共有し、（インシデント発生時に）CSP が誰に連絡すべきかを伝えます。これらのステークホルダーは、ビジネスの目的や成果物、コンプライアンスや規制の要件を強く認識する必要があります。

4.1.4 専門研究グループとの連絡

クラウドセキュリティのリスクは日々変化しており、遅れずについて行くことはほぼ不可能です。組織には、専門研究グループとの関係を確立し、維持するための担当者やチームを設置することを強く推奨します。このような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、一部の脆弱性に対して考えられる修正を提供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、（修正を探すときに）組織の時間を節約できる可能性があります。他の利点として、組織のニーズ（業界、技術、規制など）に最も関連する特定の専門研究グループを選べます。そして、これらの専門研究グループは、新しいトレンド、プライバシー、脅威、脆弱性、対策などに関する最新情報を提供することもあります。

4.2 モバイル端末とテレワーク

4.2.1 モバイル端末のポリシー

COVID-19 は、誰も予想できなかったほどの影響をもたらしました。多くの組織が、事業継続のために、在宅勤務のソリューションを急いで提供する必要がありました。

SaaS サービスは、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 サービスのネイティブ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。モバイル端末には、個人または組織支給のノートパソコン、個人または組織支給の携帯電話、またはタブレット端末があります。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、安全で継続的な事業を支えるために、ポリシー、手順、ガイドラインを作成するべきです。

CSC は、モバイル端末から組織のリソースへのアクセスを許可することによるリスクを特定するべきです。以下は、検討すべき分野の一例です。

- 誰が組織のリソースにアクセスできますか。
- 組織の社員のみがアクセスできますか。それとも、契約社員やサードパーティーのサプライヤーもアクセスできますか。
- 誰でもアクセスできる組織のリソースはありますか。
- 契約社員やサードパーティーのサプライヤーに対して、制限すべき組織のリソースはありますか。
- VPN、ソフトウェアトークン、MFA など、どのようにアクセスを付与しますか。

- 個人所有の端末から、組織のリソースへのアクセスを許可しますか。
- 個人所有の端末を許可する場合、マルウェア、フィッシング、なりすまし攻撃などから、どのように組織のリソースを保護しますか。
- 社員や契約社員にアクセスを付与した後、明示的に権限を与えたリソースにしかアクセスできないことを、どのように確認しますか。
- どのようにアクセスを監視し、記録しますか。
- 組織の機密情報や秘密が、盗まれたり、社外（もしくは、許可されていない人や競合）に持ち出されたりしないことを、どのように確認しますか。
- 社員が退職を決断した場合、その社員が組織のデータを持ち出さないように、どのような対策をしますか。

CSC が考慮すべき技術的対策の他、以下のような管理的対策も考慮が必要です（網羅的ではありません）。

- セキュリティ意識向上のトレーニング
- 利用規定
- データ分類の標準やポリシー
- 機密データや秘密データの取り扱い
- 記録媒体の取り扱い
- リムーバブルメディアの使用
- （会社支給端末の）暗号化
- （会社支給端末に対する）物理的対策
- データの保持期間と破棄

5. 資産管理

SaaS サービスの恩恵を受けるため、SaaS の利用者は、ある程度のデータを提供して SaaS サービス上で処理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 資産管理台帳

SaaS の利用者は、以下の質問に答えられるべきです。

- どのようなデータを、SaaS サービスに転送しますか。
- どのようにデータを転送しますか。
- SaaS サービスは、どのデータにアクセスできますか。
- 自組織のデータについて、SaaS サービスに何を依存しますか。
- 規制や顧客サービスの要件など、データに対して地理的な要件がありますか。
- 組織全体でいくつの SaaS アプリケーションを利用していますか。シャドーSaaS は存在していますか。
- CSC は、既に使っ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（有効な）リソースがあると、運用コストがすぐに増えてしまいます。
- CSC は、クラウドに置かれたすべてのリソースをすぐに特定できますか。CSC は、組織内に中央リポジトリを用意し、資産の所有権と責任を文書化するべきです。また、CSC は、組織全体に適用するタグ付けのポリシーとスキーマを策定するべきです。タグ付けは、CSC がクラウドに置かれたリソースを正確に追跡することを容易にし、また、地理的な位置、秘密度、法的義務、コスト最適化など、多くの属性でクラウドリソースを分類できるため、組織のセキュリティガバナンスの取り組みを支えることができます。

5.1.2 資産の発見

プロセス、もしくは、理想的にはソリューションを実装して、組織内のユーザーによる SaaS の利用を継続的に調査し、特定するべきです。これは、以下のいずれかの方法で実現できます。

- 手続きを定め、SaaS を購入または取得する場合、利用する前に、IT 部門やセキュリティ部門に通知します。
- ファイアウォール、Web ゲートウェイ、CASB のログを分析して、評価します。
- SaaS Security Posture Management ソリューションを利用します。
- 経費申請や財務記録から、SaaS に関連する項目を分析します。

5.1.3 資産の所有権

SaaS の利用者は、以下の質問に答えられるべきです。

- その SaaS サービスにどのようなデータが置かれているかについて、誰が責任を負いますか。
- その SaaS の管理者は誰ですか。

5.1.4 許容される資産の利用

これには、2 つの側面があります。

- SaaS プロバイダーは、利用者のデータやメタデータに対して、何を行うことが許可されていますか。
- SaaS サービス上のデータに対して、自組織のユーザーは何を行うことが許可されていますか。

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 アクセス制御のポリシー

- その人に、リソースへのアクセスが必要かを評価します。
- ビジネス要件と役割を明確にします。
- データ分類にもとづいて、情報へのアクセスを統制します。
- セキュリティレビューを経て、データ所有者（スポンサー）が承認します。

組織内のユーザーは、一般的に、過去からの成り行きや、同僚のアクセス権限の複製によって、アプリケーションへのアクセスを付与されます。

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かを評価して、ビジネス要件を明確にした上で、役割を設定することが重要です。

6.2 ユーザーアクセスの管理

Identity and Access Management（IAM）の適切な管理と設計は、クラウドリソースの保護に不可欠です。プラットフォームを導入する際は、セキュリティとビジネスの要件を検討することにより、職務やビジネス要件に従って、ユーザーのグループ分け、分離、必要な権限が、ユーザーに適切に割り当てられるようにすることが欠かせません。適切な IAM 運用は、最小権限と職務分掌を強制します。

6.2.1 ユーザーの登録と削除

6.2.1.1 ユーザーアクセスのプロビジョニング

- ベストプラクティスに関するユーザートレーニング
- 許容される使用、関連するポリシー、手順に対する意識向上
- ユーザーアクセスに関するベースラインに従ったアカウント作成
- 組織全体の入社、異動、退社のプロセスへの組み込み
- 可能な限り、ロールベースのアクセスを利用し、最小権限を遵守
- 用途にもとづいて、グループやスポンサーを費用負担元に設定
- リソースに対する制限の確認と設定

常に、最小権限の考え方に従います。また、リソースに対する制限を確認し、設定します。

6.2.2 特権アクセスの管理

- 特権アクセスが必要であることを確認するため、正当な理由を求めるべきです。
- 必要時のみ権限を昇格させ、その後、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。
- 特権アクセスが必要なユーザーの数を最小限にするべきです。

6.2.3 機密性の高い認証情報の管理

- 緊急時の特権アクセスは、極めて限定した目的のみに使用するべきです。その認証情報は、Key Vault など、適切なセキュリティレベルで保管するべきです。

6.2.4 ユーザーのアクセス権限のレビュー

- アクセス権限は、適切であり、ビジネスの変更と整合性が取れていることを確認するため、定期的にレビューするべきです。

6.2.5 アクセス権限の削除または調整

- アカウントを即時に停止します。
- アカウントに関連するリソースの課金を停止します。
- 監査ログやアクセスログを、ビジネスポリシーに従って保管しなければなりません。
- 必要に応じて、セキュリティレビューを実施します。
- アカウントの停止ログと管理台帳を更新します。

セキュリティポリシーに従って、監査ログをレビューし、保持します。

そして最後に、リソースが使用されなくなったら、課金を停止します。できれば、自動化し、手作業を排除します。

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もとづいて、監視アラートを設定します。
- 不審なログイン（場所、時間など）やデータアクセス（バッチアクセスなど）を通知します。
- パスワードポリシーを遵守させます。
- データ損失防止を監視します。
- 外部ユーザーや契約社員の行動と従業員の行動を区別しながら、アラートを設定し、不審な行動やログインを監視します。
- API ベースのソリューションを活用して、保存データを監視します。

6.3 システムやアプリケーションからのアクセス制御

6.3.1 情報へのアクセス制限

- SaaS アプリケーションに保存した情報は、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済デバイスから、認証済のユーザーのみがアクセスできるべきです。（外部とのコラボレーションアプリケーションなど）アプリケーションの性質上、実現できない場合は、リバースプロキシなどの他ソリューションが、必要な粒度のアクセス制御を提供できるかもしれません。
- API ベースのソリューションを利用して、保存データの保護や、適切な共有と DLP ポリシーの強制ができます（例えば、個人情報を含む文書を外部ドメインと共有した場合、自動的に組織内ユーザーのみのアクセスに戻します）。SaaS アプリケーションはインターネットに公開されているため、可能な場合は、アクセスを、承認済の IP アドレス範囲や場所からに制限するべきです。
- SaaS アプリケーションに格納した情報を（アクセス後に）ダウンロードする必要がある場合は、適切なセキュリティ管理策を導入し、ビジネスセキュリティポリシーに準拠した承認済デバイスに、情報がダウンロードされることを確認するべきです。
- SaaS アプリケーションの認可インスタンスと未認可インスタンスを区別し、それに合わせて、利用ポリシーを適用できることが重要です。
- API によるサードパーティーへのアクセスは、適切なチェックを経て、承認する必要があります。そして、ビジネス要件を満たしたら、承認を取り消す必要があります。
- SaaS プロバイダーが SaaS 利用者のデータにアクセスする必要がある場合、利用者は通知を受け、その要求を評価し、要求を承認または拒否できるべきです。

6.3.2 安全なログオン手順

- 本質的に安全でないため、Basic 認証を有効にするべきではありません。
- 可能な場合、SaaS アプリケーションは、利用者の Identity Provider を使用し、Single Sign-On（SSO）による安全なログオンを使うべきです。
- SSO が使えない場合、SaaS アプリケーションは、複雑かつ未公開のパスワードを強制するべきです（例えば、https://haveibeenpwned.com/で検証します）。このパスワードは、組織内で使うパスワードと異なるべきです。
- SaaS アプリケーションはインターネットに公開されているため、ユーザーが本人であることを確認するため、多要素認証を導入するべきです。
- 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デバイスからのみ、SaaS アプリケーションにログインするべきです。
- 安全なログインに失敗した場合、パスワードリセットの手続きは、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

- 可能な場合、SaaS アプリケーションでパスワードを管理せず、代わりに、利用者の Identity Provider を利用

して SSO でユーザーを認証するべきです。
- ローカル認証を使用する場合、パスワードは OWASP が定める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、Key Vault もしくは同様のセキュリティデバイスに保管するべきです。

パスワードは、「認証情報」であることに留意してください。「認証情報」には、暗号鍵、デジタル証明書、トークンなどの形式もあります。CSC が鍵を管理できない場合、機密性、完全性、可用性を確保するため、Key Vault もしくは同様のセキュリティソリューションを利用することが強く推奨されます。

6.3.4 特権的な管理プログラムやサードパーティープラグインの使用

- プログラムからの Basic 認証を許可するべきではありません。
- 呼出元のアイデンティティを mTLS によって検証するべきです。
- トークンベースの認証フロー（OAuth 2.0）を推奨します。
- SaaS API は、指定した IP アドレス範囲からのみ利用できるべきです。
- 安全な保管場所を用意し、特権の認証情報を暗号化して保管します。
- API の鍵を安全に保管し、送信時は HTTPS を使うべきです。
- SaaS アプリケーションは、アクセスキーとトークン付与を取り消す機能を持つべきです。
- 特権的なプログラムのアクセスに使うアイデンティティは、定期的にレビューするべきです。
- サードパーティーアプリケーションに、ユーザーが付与した同意をレビューします。
- サードパーティーアプリケーション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 プロバイダーに制限するべきです。
- ソースコードを生成する開発パイプラインや環境へのアクセス制御も、SaaS プロバイダーに制限するべきです。
- ソースコードは、SaaS プロバイダーの制御下にない、もしくは SaaS 利用者向けの設定の一部ではない、他のプログラムやシステムへのバックドアアクセスを提供するべきではありません。
- 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できるべきです。
- CSC は、どのようなセキュリティゲートを実装するか、また、CI/CD パイプラインを使う場合、どのイベントがセキュリティレビューを開始するかを説明するプロセスを文書化するべきです。セキュリティゲートは、ソフトウェアコード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です。次のフェーズに進む前に、すべてのソフトウェアコードをレビューし、承認しなければなりません。

7. 暗号化と鍵管理

7.1 SaaS 環境内にあるデータのセキュリティ

SaaS サービスを利用する際に最も重要な側面のひとつは、そのサービス内に保存す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、アプリケーションセキュリティの多くに責任負います。しかし、責任共有モデルで分かるように、データはクラウド利用者の責任です。

SaaS プロバイダーへのデータ転送やデータ保存における安全性を確実にするため、データの暗号化とそこに使われる暗号鍵の管理は、ベンダーを利用するにときに、利用者が考慮するべき領域です。データが社内の安全な場所から移動すると、利用者組織には、そのデータが意図せず、または、悪意によって外部に公開するリスクが発生します。適切な暗号化と鍵管理を徹底することは、万が一、不正なデータアクセスが発生しても、まず復号しない限り、そのデータを利用できないことを意味します。

この章では、SaaS プロバイダーに保存したデータが、管理の行き届いた暗号鍵を使って、適切に暗号化されることを確実にするため、利用者組織が行える手順を説明します。

7.1.1 責任共有モデル

SaaS サービスの利用は、アプリケーションの管理や維持のための責任の一部を、利用者組織からベンダーに移しますが、一部の責任は利用者に残ります。利用者に残る責任には、SaaS サービス内のデータのガバナンスとセキュリティ、および、SaaS サービス内のアクセスモデルを含みます。

	責任	SaaS	PaaS	IaaS	オンプレ
常に利用者が保持する責任	情報とデータ	🔵	🔵	🔵	🔵
	デバイス（モバイルと PC）	🔵	🔵	🔵	🔵
	アカウントとアイデンティティ	🔵	🔵	🔵	🔵
サービス種類によって異なる責任	アイデンティティとディレクトリインフラ	🟠🔵	🟠🔵	🔵	🔵
	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	🟠	🟠	🔵	🔵
クラウドプロバイダーに移転する責任	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 プロバイダーと共有するデータの暗号化

前述したとおり、データが社内の安全な場所から移動すると、意図せず、または、悪意によって外部に公開するリスクが発生します。このリスクを軽減するための考えられる最善の方法は、SaaS プロバイダーとの間で転送するデータと、SaaS プロバイダーのシステムに保存するデータの暗号化を確実にすることです。これには、アプリケーション内や物理リソース内での適切な暗号化の実施といった、SaaS プロバイダーの責任を含みます。

7.2.1 検討すべき質問と領域

必要な暗号化のレベルと暗号化が必要な場所は、転送するデータと SaaS プロバイダーの運用によって変わります。下記は、組織のデータに必要な保護のレベルを決定する際に検討すべき質問です。

7.2.1.1 ベンダーへの質問

- ベンダーは、データ共有のための詳細な制御を提供していますか？（例えば、組織内のみの共有、選択したパートナーとの共有、すべてのユーザーとの共有など）
- SaaS プロバイダーは、転送中のデータの暗号化を提供していますか。
- SaaS プロバイダーは、保存データの暗号化を提供していますか。
- SaaS プロバイダーは、エンドツーエンドの暗号化をサポートしますか。
- SaaS プロバイダーは、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ますか。
- SaaS プロバイダーは、利用者（テナント）ごとに、個別の暗号鍵を提供していますか。
- SaaS プロバイダーは、プロバイダー内の鍵管理手順に関する文書を用意していますか。
- SaaS プロバイダーは、利用者管理の暗号鍵の使用を許可していますか。
- SaaS プロバイダーは、機微なデータを特定したり、マスキングしたりする機能を用意していますか。
- SaaS プロバイダーは、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、仮名化したり、適切に情報を除去したりしていますか。
- SaaS プロバイダーは、機微なデータやフィールドにユーザーがタグ付けする仕組みを提供していますか。

7.2.1.2 組織内への質問

- SaaS プロバイダーにアップロードするデータに、機微な内容が含まれていますか。
  - 機微なデータには、個人情報や、組織のデータプライバシーやコンプライアンスの要求事項が定める他要素を含みます。
- データが外部に公開された場合、利用者組織にどのような影響がありますか。
- 組織内に成熟した鍵管理の運用が存在しますか。
- 組織内のプロセスは、エンドツーエンドの暗号化をサポートしますか。

7.2.2 転送中の暗号化

データがある場所から別の場所に移動することを「転送中」と考え、これには、利用者組織と SaaS プロバイダーの間の移動

を含みます。データセキュリティは、相互運用可能な複数の層で構成したときに最も強固になります。したがって、データの転送中は、一般的に、データを保護する層が少ないため、データセキュリティが弱くなります。

転送中のデータを保護するには、すべてのデータ転送に対して、安全な暗号ネットワークプロトコルを使用することが推奨されます。執筆時点で使える最良の暗号ネットワークプロトコルは、Transport Layer Security（TLS）のバージョン 1.2 以上です（TLS 1.3 が推奨）。概要として、TLS プロトコルは、共通鍵暗号（同じ鍵をデータの暗号化と復号に使用）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）を組み合わせて使います。このような暗号化方式の組み合わせは、転送中のデータの機密性と完全性を強化します。

TLS 1.3 は、セキュリティを犠牲にすることなく、性能のために TLS 1.2 のいくつかの手順を取り除いています。TLS 1.2 と 1.3 において、TLS ハンドシェイクと鍵交換のプロセスは、下図のように動作します。

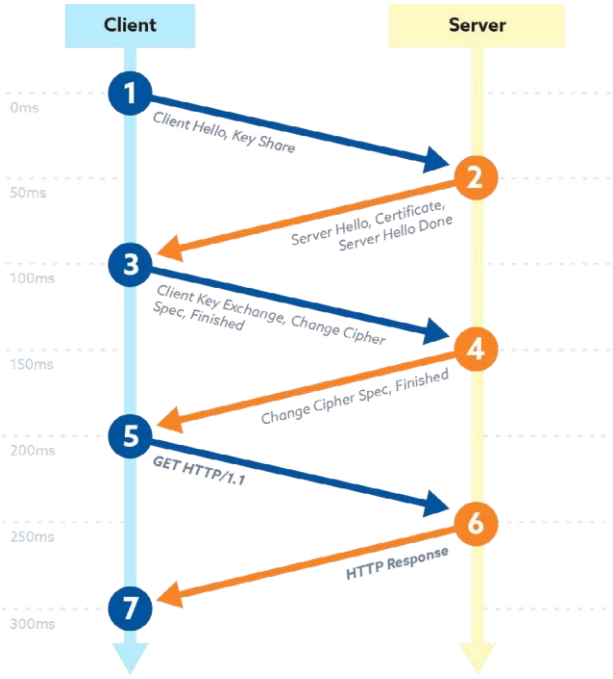

図 3. TLS 1.2（フルハンドシェイク）

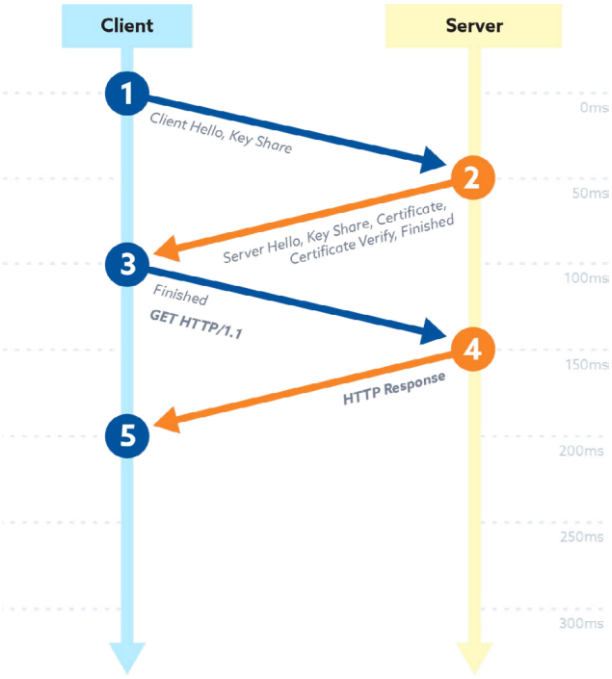

図 4. TLS 1.3（フルハンドシェイク）

7.2.3 保存中の暗号化

データがアプリケーション、ネットワーク、システム内で移動していない場合、「保存中」と考えます。「保存中」の期間に、適切に保護しない場合、SaaS プロバイダーのホスティング施設に不正アクセスした攻撃者が、データを一般に公開したり、利益のために使ったりする可能性があります。保存データの暗号化は、仮にデータを保管するハードウェアが盗まれても、そのデータを使えないようにします。

データはアプリケーション自身でも暗号化ができ、（その利用者のみが復号できるようにして）SaaS 利用者に自組織のデータのみを見せることにより、マルチテナントの SaaS プロバイダー環境に利用者間の境界を提供することができます。

暗号化の種類と強度は、データの分類に依存します。保存データが公開済の場合、機微と分類されるデータほど厳格な暗

号化は必要ないかもしれません。そのため、利用者組織は、SaaS プロバイダーにデータを保存する前に、以下の点を検討するべきです。

- データ公開についての Business Impact Analysis（BIA）
  - データを保存中に暗号化する必要があるかを決めるため、組織は BIA を実施して、そのデータが一般公開された場合の影響を理解するべきです。
  - さらに、アクセス管理など、CSP が提供する他のセキュリティコンポーネントを考慮して、データ公開のリスクを決めるべきです。
- 保存中の暗号化サービスの利用可否
  - すべての SaaS プロバイダーが、保存データの暗号化を無償で提供するわけではありません。保存中の暗号化に必要なライセンスモデルを理解する必要があります。
- 保存バックアップデータの暗号化の利用可否
  - 多くの SaaS プロバイダーが保存データの暗号化を提供しますが、データのバックアップにも適用されるとは限りません。意図的に保存したデータとすべてのバックアップが、保存中に暗号化されるようにしてください。
- ディスク全体の暗号化とファイル単位の暗号化の比較
  - 提供される保存中の暗号化の種類を理解してください。例えば、ディスク全体の暗号化は合理的な管理策ですが、主にディスクやシステムの盗難に対する保護に使います。
  - より一般的なシナリオとして、ファイルベースの暗号化は、不正アクセスがあった場合に、個々のファイルやデータを盗難から保護します。
- 保存データの暗号化に使う暗号化アルゴリズムと鍵の長さ
  - 保存データの暗号化方式が、CSC の要求事項を満たすか確認してください。NIST 800-57 Part 1: Recommendation for Key Management（Table 2 を参照）は、アルゴリズムと鍵の長さによる暗号強度をまとめています。

7.3 暗号鍵の利用者管理とベンダー管理の比較

一般的に、利用者管理の暗号鍵を使った方が、ベンダー提供の暗号鍵より安全です。しかし、ベンダー管理の暗号鍵を使うかは、2 つの要素に依存します。まず、ベンダーは、利用者管理の鍵の使用を許可していますでしょうか。すべてのベンダーが、利用者の暗号鍵を使うための機能を提供するわけではありません。次に、ベンダーに保存するデータは、利用者の鍵を使ったリスク軽減のレベルを必要としますでしょうか。それとも、ベンダー管理の鍵を使うリスクを許容できますでしょうか。

例えば、ベンダー管理の暗号鍵を使うことによるリスクは、以下の質問への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の方法について、情報を提供していますか。
  - 多くの場合、ベンダーは、ベンダー環境内での、暗号鍵の作成とライフサイクル管理の詳細を共有しません。
  - ベンダーによる暗号鍵の作成と管理の運用を確認するため、ベンダーのシステムで転送中や使用中のデータをどのように暗号化するかについて、文書の提供を要求することを推奨します。
- ベンダーのシステムに保存するデータは、どのくらい機微ですか。
  - 例えば、一般公開データは、ベンダー管理の暗号鍵を使ってもほとんどリスクがありません。
- 自組織に、適切な暗号鍵管理の運用がありますか。

- ベンダーのセキュリティに加えて、鍵管理によって提供される保護は、自組織の鍵を保護する能力にも依存します。自組織の運用がベンダーと比較して未熟な場合は、ベンダー管理の鍵を使った方が良いかもしれません。

7.4 暗号化と鍵管理の今後

今後の検討領域です。

- Hardware Security Module as a Service（HSMaaS）
  - 「クラウド HSM」とも呼ばれ、SaaS 提供の HSM サービスを利用して、暗号鍵の作成や管理を行います。
  - まだ普及が進んでいませんが、Fortanix や Microsoft など、FIPS 検証済の HSMaaS プロバイダーの利用が増えています。
- Privacy-Enhancing Cryptography（PEC）
  - 機能を維持しながら、システムが収集する個人情報や機微な情報を最小限に抑える、一連の技術です。
  - 一般化したサービス提供のため、SaaS プロバイダーは、PEC 技術の使用をサポートしないかもしれません。PEC 技術には、多くのカスタマイズやユーザーシステムとの連携が必要です。
  - NIST は、PEC 技術を評価するブログ記事やプロジェクトを提供しており、関連する標準や要件をまとめています。
- 準同型暗号（Homomorphic Encryption）
  - データを暗号化したまま使用し、ビットレベルでの暗号化と復号により、データ操作を可能にします。従来の方式と比較して非常に遅いです。
  - 準同型暗号を含む、PEC 方式の要件の文書化は、オープンコンソーシアムによるリーダーシップのもと、ISO や NIST などの組織が現在も開発しています。
- Confidential Computing、または、Secure Enclave
  - ハードウェア機能を使って、他の並列ワークロードから分離して処理することにより、使用中のクラウドデータを保護します。
  - NIST は、クラウドやエッジコンピューティングにおける、Confidential Computing 技術についてドラフト文書を提供しています。
- ポスト量子暗号化（Post-Quantum Cryptography）
  - 少なくとも、まだ 8 年以上先と思われます。
  - 2016 年の NIST Internal Report (IR) 8105 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 年まで出現する可能性があると呼びかけています。
  - NIST などの組織は、ポスト量子暗号の標準策定に向けてプロジェクトや取り組みを進めており、そのいくつかでは、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 運用手順の文書化

SaaS 製品には自由度があるため、組織がその製品をどのように使っているかを把握する必要があります。

- アクセス制御 - 「6. アクセス制御」を参照
- 変更管理
- キャパシティ管理
- 環境の分離
- 契約解約 - 「3.1.3. 解約」を参照

8.1.2 変更管理

SaaS 製品の追加は、慎重に検討するべきです。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べきです。SaaS 製品には、小さな変更が頻繁に行われる傾向があります。多くの場合、ユーザーは、その変化に気づかれないかもしれません。一方で、周辺システムが影響を受ける可能性があります。

変更が、組織のセキュリティ態勢に影響を与えるかを特定することが重要です。このような変更によって、組織は他システムを修正する必要があるかもしれません。バージョンアップのような大きな変更は、レビューを実施し、変更管理プロセスに含める必要があります。

さらに、SaaS 製品は、特定の業務範囲の中で使うことを前提としている場合が多いです。その後、SaaS アプリケーションのビジネス機能の変更や、利用の拡大、利用方法の変化によって、SaaS アプリケーションの使用にともなうセキュリティを再検討する必要が生じる可能性があります。管理者が SaaS アプリケーションの利用状況を定期的にレビューし、初期のセキュリティレビューの範囲が現在の利用範囲にも合致することを確認することを推奨します。これにより、SaaS アプリケーションのセキュリティモデルを最新の状態に維持します。

8.1.3 キャパシティ管理

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かもしれません。監視製品にも、監視または接続できるアカウント数に制限があるかもしれません。ユーザー数やアカウント数によって、価格が変わるかもしれません。利用を拡大する前に、要求事項を把握する配慮が必要です。

8.1.4 開発、テスト、本番環境の分離

社内で開発するシステムと同様に、本番データが本番用途のシステムの外に出ないように、環境を分離する必要があります。SaaS ベンダーは、継続的にシステムを改良すると想定されます。改修、アップグレード、アップデートは、非本番環境で、非本番データを使ってテストするべきです。SaaS ベンダーは、非本番環境が存在することだけでなく、これらの環境に非本番データしか存在しないことを証明するべきです。

さらに、SaaS アプリケーションの構成を継続的に評価して、安全な環境を維持するべきです。ユーザーやサードパーティー統合における、セキュリティ設定やデータアクセスの設定ミスを特定することにより、データ漏洩が起きるリスクを軽減します。ステージング環境と本番環境を使った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行い、本番環境に影響する前に、セキュリティの課題を特定するべきです。

8.2 マルウェアからの保護

8.2.1 マルウェアに対する管理策

マルウェア対策に関する責任の多くが SaaS プロバイダーにありますが、それでも、いくつかのマルウェア配布の経路は、SaaS のユーザーや管理者の管理下に存在します。このようなユーザー管理下の経路の例には、カスタマイズできる静的ファイルホスティングと添付ファイルがあります。そこには、組織の従業員が SaaS のアプリケーションユーザーや特権ユーザーを使ってアップロードしたり、SaaS アプリケーションがポータルを一般公開する場合は、不特定多数がアップロードしたりするかもしれません。

SaaS 管理者とセキュリティ部門は、一般的な脅威モデリングを実施し、存在する場合は、一般公開する SaaS の機能が含むコンテンツアップロード機能を把握するべきです。一般公開するコンテンツやドキュメントのアップロードシステムに注意してください。そこに保存または転送したファイルは、SaaS アプリケーションの組織内ユーザーや特権ユーザーが、会社の端末にダウンロードしたり、参照したりします。

SaaS とその構成を評価する際、利用者は SaaS プラットフォームの組み込み機能を理解するべきです。多くの場合、標準的なマルウェアやウイルスのスキャン機能があり、悪意のある可能性があるアップロードにフラグを立てたり、アップロードをブロックしたりします。SaaS システムの構成は、（1）外部からアップロードできるコンテンツの種類と量を最小限に抑え、（2）プラットフォーム組み込みの保護やファイル種類の制限が有効になるように、評価および監視するべきです。

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 プロバイダーにあります。これは、SaaS 利用者がデータベースへの直接的なアクセスや、フェイルオーバー用のインスタンスやレプリカを作成する権限を持たないため、妥当な責任分担です。利用者のデータアクセスは、一般的に、SaaS プラットフォームがサポートする API に限定され、データバックアップの作成や管理には非効率です。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ーがデータの復元に責任を負います。このため、SaaS の管理に

おける情報のバックアップは、利用者が下位のレイヤーを制御する IaaS などに比べて、重要な考慮事項ではありません。

それでも、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があります。SaaS アプリケーションが想定かつ許容する範囲内で、不注意や悪意によってデータが削除された場合（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）、SaaS プロバイダーは、バックアップの提供やバックアップからのリストアに責任を持ちません。利用者が SaaS アプリケーションを管理する経験則として、プラットフォームが設計通りに動作している限り、例え、構成が安全でなく、誤っていても、SaaS プロバイダー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、継続的な構成とデータアクセスの監視を導入して、データの損失を引き起こす可能性がある、不注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ことが重要です。ユーザーに適切な最小権限を付与するようにデータアクセスを管理したり、システム構成を監視して、容易なデータ復元のため、論理削除やデータ保持が有効になっていることを確認したりするかもしれません。最後に、SaaS プロバイダーが、まだ、ロールバックやバックアップのソリューションをプラットフォームに提供していない場合、SaaS 利用者は、プラットフォーム外に、追加の API ベースのデータバックアップソリューションを導入し、重要データの冗長性を高められるか検討するべきです。

データのバックアップの他、CSC は、スナップショットの戦略を実装するべきです。NIST Standard 800-125 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します。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、バックアップからのリストアと比べて、イメージやデータのリストアを短時間で行えることです。

8.3.1.1 高可用性

多くの SaaS プロバイダーは、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。その一方で、SaaS 利用者は、SaaS アプリケーションに対する要件に従って、他の冗長性のオプションを選択するかもしれません。SaaS だからと言うだけで、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べきです。

8.4 ログと監視

8.4.1 イベントログ

SaaS のイベントログとアクセスログは、セキュリティチームが慣れ親しんできた、インフラ、IaaS、PaaS、アプリケーションなどの伝統的なログ出力とは、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部門の観点からは、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利用と管理を監視するセキュリティチームは、定義上、SaaS プロバイダーが提供するログの利用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、手動のリクエストプロセスによって、SaaS プロバイダーから追加費用で入手できる場合がありますが、タイムラグや、手間、費用のため、SaaS のログ監視プログラムのベスト

プラクティスではありません。

セキュリティ部門が SaaS アプリケーションのセキュリティを監視する難しさに加え、SaaS アプリケーションのログ出力には、業界標準として受け入れられたフォーマットが存在しません。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 アプリケーションごとに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横断してログやアクティビティを関連付けたいセキュリティ部門にとって課題です。

また、ログが提供されるタイミングは、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部門にとって課題となる可能性があります。ログのエントリーは、SaaS プロバイダーが処理をして、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できません。SaaS プロバイダー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る可能性があります。

これらの複雑さは、SaaS イベントログを、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使う際の課題になりますが、SaaS セキュリティソリューションの一部として、SaaS イベントログの監視に価値がないわけではありません。SaaS イベントログを扱うセキュリティ部門は、以下の機能を、開発または導入するべきです。

- SaaS アプリケーションやプロバイダーからのログ取得を、高い頻度で自動化するべきです。
- SaaS のログは、SaaS アプリケーション間で共通フォーマットに正規化してから、SIEM や他のログ保管ソリューションに配信するべきです。これにより、セキュリティチームは、複数の SaaS アプリケーションを横断して、効果的にアクティビティを監視することができます。
- イベントログ、監査ログ、アクティビティログ、およびその他のログのエントリーが、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、組織内で使っているアイデンティティに正規化し、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するべきです。
- SaaS アプリケーションごとに、イベントの発生からログの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、ログシステムを使うセキュリティ運用チームが理解できるようにするべきです。

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構成変更を監視するために、専用のログや監査機能を備えています。この機能は、「監査証跡」や「セットアップログ」など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であり、異なる API やアクセス方法を使って取得することがあります。

これらのログには、SaaS イベント監視プログラムの一部としてアクセスすることが重要であり、SaaS アプリケーションのセキュリティ態勢に重大な影響を与える恐れがある、特権によるアクションを記録します。これらのログも、「8.4.1 イベントログ」で説明したすべてのベストプラクティスに従うべきです。

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、一連のログの中から懸念されるアクションの種類を特定し、それらを監視することにより、特権ユーザ（SaaS 管理者など）によるセキュリティに影響する変更を、セキュリティチームに通知で

きる、自動化されたセキュリティ技術の導入を検討するべきです。事前定義した「高リスク」の行動を、複数の SaaS エコシステムを横断して監視することにより、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をつないでください。多くの組織で、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に含まれます。一方、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定義します。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、脆弱性管理の責任を定義することが重要です。

複数の SaaS アプリケーションを横断して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 プロバイダーのインフラ内で発生した場合、SaaS 利用者は、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。利用者の責任には、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 などの標準と比較して構成をレビューすることは、コンプライアンスに沿わない、もしくは、安全でない構成のリスクを避け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、より耐性のある暗号を使用するように、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、影響を軽減することができます。他にも、管理者が重要なセキュリティ保護メカニズム（クロスサイトスクリプティング保護など）を無効にして、ユーザーにより良い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誤った設定に対する警告を受け、この問題を修正するべきです。

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、部門横断的な協力がないと、最大の効果を発揮することができません。IT アプリケーションの所有者が問題に対応しなければなりません。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わなければなりません。他のセキュリティ領域と同様、組織内で承認された SLA に合わせて、それに従うことが重要です。

Cloud Security Alliance のブログ記事「Building a SaaS Security Program: A Quick Start Guide」は、次のように説明します。「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 のワークフローであっても、最も緊急なセキュリティの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、すべてのセキュリティに関する脆弱性を棚卸し、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し、最も重要な問題を最初に修正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 プロバイダーは、利用者の情報システム監査の統制下にないかもしれません。しかし、利用者は、（通常、規制によって）SaaS プロバイダーが許容できる管理策を実装していることの保証を求められます。これに対して、プロバイダーの自己評価や、第三者認証を使うことがあります。

自己評価の利用は、法律に応えるための最低限のレビューですが、実装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を把握するには、最も信頼性が低い方法です。同様に、下記に注意して、第三者評価を注意深く読み込むことが重要です。

- アセスメントのスコープ - 追加の IaaS、PaaS、SaaS、それ以外の第四者のソリューションなど、アセスメントのスコープに含まれない第四者が存在し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、管理台帳、およびアセスメントのスコープと深さを、十分に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、第三者のアセスメント（ISO 27001、SOC 2 Type 2）に頼る場合、熟練したレビュアー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レビュアーが望ましいです。
    - 第三者のアセスメントによって、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、サンプルの収集と検証が行われたことを確認できます。
    - 監査人の習熟度が、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「問題なし」と記載され、テスト方法の記述がない、もしくは不明瞭な場合、その内容を使うべきではありません。

この問題は、受け入れ可能な個別の標準（CSA CCM、FedRamp、NIST、ISO など）に SaaS プロバイダーが従うことを求め、それらの標準に対する証明と、管理策の有効性を示す定期的なレビュー結果の提供を、契約条項に含めることで解消できるかもしれません。

Cloud Security Alliance 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 による監査を手引きすることを目的としています。監査人には、CCM v4.0 の管理策の仕様ごとにアセスメントガイドラインが提供され、より監査がしやすい管理策を実装し、組織がより効率的に遵守できるようにすることを目的とします。このガイドラインは、網羅的でも慣例と認められたものでもありません。一般的な手引きとして、アセスメントの推奨事項をまとめています。監査人は、監査の目的に合わせて、説明、手順、リスク、管理策、文書などをカスタマイズし、アセスメント対象の組織やサービス向けに監査プログラムを用意する必要があります。

9. ネットワークセキュリティ管理

データフローのセキュリティに関連するネットワークセキュリティや管理策のガバナンスは、SaaS サービス利用の文脈において、SaaS プロバイダーが所有および運用する管理策と、SaaS 利用者が考慮する管理策の 2 つの領域に分類されます。

いずれの領域にもまたがる重要なネットワーク管理策は、転送中のデータの暗号化、特定リソースへのアクセス認可、データ転送の制御に集約されます。

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 のアプローチを説明します。

9.1 SaaS プロバイダーによるネットワーク制御

サービス利用者は、SaaS プロバイダーに、外部からの接続や、内部のマイクロサービスの保護に有効な TLS 証明書を利用していることを確認するべきです。証明書は、よく知られた、信頼できる認証局が発行するべきで、自己署名であるべきではありません。

さらに、サービス利用者は、SaaS プラットフォーム内の個々のサービスコンポーネント間において、暗号化が利用されている範囲を確認するべきです。

SaaS プロバイダーは、最小権限にもとづく Zero Trust Network Access ポリシーによって、ネットワークのデータフローを制御することがあります。SaaS プロバイダーは、発見的管理策として、ネットワークフローによる異常検知を利用することがあります。

9.2 SaaS 利用者によるネットワーク制御

サービス利用者は、SaaS プロバイダーに関連する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策を考慮するべきです。

SaaS プロバイダーへの接続はインターネットを経由することがあるため、TLS 1.2 以上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策です。

SaaS サービスへのアクセスは、悪意のある行為者に対して、SaaS 利用者の管理下にないアカウントにデータをアップロードすることにより、データを持ち出す機会を与えることがあります。Cloud Access Security Broker（CASB）とテナント単位の認証制御を使って、このリスクを制御します。

Data Loss Prevention（DLP）による管理策も検討するべきです。これらは、ペイロードデータへのアクセスに応じて、ネットワーク、もしくは、他の層に導入することがあります。

サービス利用者は、SaaS プロバイダーとのネットワーク接続を設計する際に、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、可用性要件を検討するべきです。

SaaS の利用者は、Protective DNS（多くの場合、SaaS ベースのサービス）を使った DNS トラフィックの制御を検討するべきです。

現代のネットワークアーキテクチャーは、アウトバウンドのインターネットアクセスを分散させ、各拠点からインターネットブレイクアウトを利用することがあります。SaaS 利用者は、SaaS サービスを直接利用する場合[3]であっても、前述した管理策を適用しなければなりません。

Secure Access Service Edge（SASE）モデルは、SaaS 利用者とプロバイダーの間で、ポリシー実施ポイントとして機能することにより、このような制御を容易にできることがあります。

[3] 訳注：データセンターを経由せず、直接インターネット経由でアクセスする場合

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 製品のほとんどは、第三者のサービス上に構築されており、サプライヤーが直接、管理、維持するサービスだけでなく、第四者[4]の IaaS、PaaS、SaaS も含みます。従来の利用者が管理するソフトウェア展開とは異なり、SaaS の利用者は、対象となる製品の完全な依存関係を把握することが難しい場合が多いです。そのため、SaaS 製品を運用する組織にとっては、自組織のビジネスオペレーションが依存する技術について包括的なモデルを構築することが重要です。

従来の利用者が管理するソフトウェア展開と同様、SaaS に対して、SaaSBOM とも呼ばれるソフトウェア部品表（Software Bills Of Material; SBOM）を整備することにより、このようなモデルが提供できます。既存の標準である CycloneDX を使って、SaaS のコンポーネントを含めた SBOM を作成することができます。このような記述を評価することにより、組織は、技術のサプライチェーンに潜む既知の脆弱性を特定し、より速く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のリアルタイムな状態を作成し、維持することに加え、組織は、その SaaS 製品を利用するための組織内のリスクマネジメントポリシーを策定するべきです。同様に、組織は CSP と契約条件を交渉し、そのサービスのセキュリティを確保するべきです。最後に、外部認証の制度は、リスクマネジメントの分析や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のための情報セキュリティポリシー

ビジネスオペレーションの一部を他者に依存するすべての組織、つまり現代経済におけるすべての組織は、サードパーティーリスク管理のポリシーを実装するべきです。組織が直接関係を持つ第三者だけでなく、これらの外部の組織自身が関係性のネットワークを持ち、第四者に依存するため、サードパーティーリスク管理のポリシーが必要になります。

このポリシーは、組織が依存する他の技術に加え、SaaS 製品にも適用するべきです。少なくとも、このようなポリシーは以下を明確にします。

- 第三者との関係（および内在する第四者リスク）毎に、組織内で説明責任を持つ唯一の役割や役職
- 第三者の製品やサービスに依存するビジネスオペレーションの重要性について、できれば定量的に、上記の個人が書面によるアセスメントを提供するという要件
- インシデントがこの第三者に影響する可能性と、そのインシデントが組織のビジネスオペレーションに与える影響を、上記で明確にした重要性を踏まえて評価する方法論。これに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。
    - 外部監査とセキュリティレビュー（詳細は、認証による保証の項を参照）
    - セキュリティスコアリングや格付けを提供するベンダーのツール
    - 利用者組織による監査、ペネトレーションテスト、プロバイダーの製品やインフラに対するツールによる自動ス

[4] 訳注：自組織と直接契約関係のない再委託先

キャンなど、直接的かつ技術的なデューデリジェンス

- 上記にもとづいてリスクの閾値を設定し、第三者がこれを超えた場合に、（契約上の義務により）第三者側で、（何らかの補完的な管理策により）組織自身で、もしくはその両方で是正措置を実施
- 上記の閾値以上のリスクを受容する権限と説明責任を持つ組織内で唯一の役割や役職、ならびに、こ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 サプライヤーとの契約で行うセキュリティ対応

サプライヤーとの契約では、サプライヤーが安全で信頼できる SaaS 製品の運用を実現するように、さまざまな対策を要求するべきです。SaaS プロバイダーは、組織の規模や複雑さがさまざまであり、その提供サービスの重要さは、利用組織ごとに異なることがあります。そのため、個々のサプライヤーに合わせて契約を調整する必要がある場合があります。このような契約には、以下を含みます。

- （アップタイムとも呼ばれる）製品の可用性だけでなく、製品が扱うデータの機密性と完全性を含むサービスレベル合意書。例えば、双方の動機を適切に調整するため、特定の種類のレコードが悪意のある人物によって公開または破壊された場合、事前に定めた金額をそれらのレコードに対して支払うことに同意することを、組織はベンダーに求めることがあります。
- サプライヤーの組織が、監査やペネトレーションテストなど外部による検証を受け、その結果を提供するという要件
- 利用者組織が特定した、サプライヤーの製品内にある脆弱性を、客観的なリスクスコアリングシステムにもとづく時間内に、解決する、もしくは軽減策を明確にするという要件
- サプライヤーが脆弱性を特定し、その脆弱性の重大度や攻撃可能性を、利用者組織が補完的な管理策によって削減できる場合、サプライヤーが所定の時間内に利用者組織に通知するという要件
- 利用者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および是正において、サプライヤーが利用者組織に協力するという要件
- サプライヤーが新設するデータセンターの立地を通知するという要件、および望ましくない立地を拒否する権利

サプライヤーと交渉する組織は、自組織のリスクマネジメントに慎重に取り組み、不用意な条件を契約に追加することを避けるべきです。例えば、サプライヤーのネットワーク、システム、ソフトウェアに見つかった「すべて」の脆弱性を利用者組織に通知するという要件を定めると、アラートの嵐が発生し、対策を講じる上で本質的に役に立ちません。

10.1.2.1 外部認証

外部認証は、プロバイダーが所定の要件を満たすことを、信頼できる外部組織が保証することによって得られます。このような認証は、CSP のリスクアセスメントを支援し、またプロバイダーが主張する管理策と実際のセキュリティ態勢の比較に役立ちます。それでも、外部組織による認証結果のレビューは補完的なものであり、包括的で広範囲なサードパーティーリスク管理プログラムの代替にすべきではありません。

すべての認証や監査報告書が同じというわけではなく、また同じ種類の報告書であってもスコープが同じであるとは限りません。ISO/IEC 27001 などの認証は、規定された一連の管理策に従って、CSP が情報セキュリティ管理のベースラインを確立していることを表明します。

一方、SOC 2 の証明は、プロバイダーが規定した管理策を、プロバイダーが遵守できているかについて、監査人が評価することにもとづいています。ISO/IEC 27001 とは異なり、厳密には、SOC 2 の報告書は「認証」ではありません。監査人は、（プロバイダーが選択した）調査範囲に含まれる Trust Services Criteria に対して、プロバイダーがこれらの基準の要件を満たしているかについて、4 種類の意見のいずれかを表明します。監査人の報告書には、プロバイダーが実装していると主張する管理策からの逸脱も記載されます。多くのベンダーが「SOC 2 準拠」と主張しますが、これは監査による結論ではありません。SOC 2 の報告書をレビューする場合は、必ず以下の点を確認してください。

- TSP のどの基準（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）が考慮されているか。
- 報告書の種類はどれか。
  - SOC 2 Type 1 - TSC にもとづいて、サービスを提供する組織のシステムとその管理策の設計を言明します。報告書には、現在のシステムと実装されている管理策、およびこれらの管理策に関する文書に対して行ったレビューが記載されます。管理、技術、論理のすべての管理策を対象に、ある時点における設計を検証します。
  - SOC 2 Type 2 - サービスを提供する組織のシステムが関連する管理策を設計し、適用しており、それらの管理策が有効であるかを言明します。SOC 2 Type 2 の監査では、少なくとも 6 ヶ月分の証跡を収集して分析し、サービスを提供する組織の経営者が説明する通りに、システムや導入した管理策が機能しているかを確認します。通常、SOC 2 Type 2 の報告書は、MNDA[5]とともに共有します。
  - SOC 3 - 公開された共有可能な報告書で、SOC 2 Type 2 の報告書に類似した内容です。
- 独立した監査人によるコメントを必ず読んでください。監査人は、準拠していない領域について言明することがあります。これにより、SaaS プロバイダーがポリシーや手順の中で主張していることが実践されているか分かります。

CSP のどの報告書をレビューする場合でも、その認証や証明が対象とするスコープと事業体に細心の注意を払うことが必要です。スコープには、検討または利用している SaaS サービスが含まれるべきであり、事業体は、これから契約を締結する相手であるべきです。例えば、ベンダーによっては、自組織の管理策をレビューした報告書ではなく、サービスが稼働している IaaS プロバイダーの SOC 2 報告書を提供しているかもしれません。このような報告書は、第四者のリスク分析には有用ですが、このプロバイダー自身のレビューには使えません。

同様に、報告書のレビューを通して、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がスコープに含まれているかを判断する必要があります。

以下は、完全ではありませんが、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、認証、および証明のリストです。

- 総合的
  - American Institute of Certified Public Accountants (AICPA) - SOC 2
  - International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) - 27001
  - HITRUST - Common Security Framework (CSF)
- 政府主導

[5] 訳注：Mutual Non-Disclosure Agreement

    - アメリカ - FedRAMP
    - シンガポール - SS584
    - EU - General Data Protection Regulation
- クラウドセキュリティ関連
    - Cloud Security Alliance - STAR
    - ISO/IEC - 27017
- 金融取引関連
    - BSI Kitemark - Secure Digital Transactions
    - Payment Card Industry - DSS
- プライバシー関連
    - ISO/IEC - 27018

11. インシデント管理

11.1 クラウドが関わる情報セキュリティインシデントの管理

多くの組織がクラウドファースト戦略を掲げています。この戦略はビジネス主導の決定であることが多いですが、このような組織は、この戦略に合わせて、基礎的な情報セキュリティのプロセスと手順を見直し、適応させ、そして導入しなければならないことを認識しなければなりません。これらの重要な文書のひとつが、セキュリティもしくはサイバーインシデントの対応計画です。健全なセキュリティガバナンスの一環として、既存のインシデント対応のプロセスと手順を見直し、ビジネスが利用するクラウドコンピューティングのすべてのサービスモデルと展開モデルを組み込むべきです。

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

11.2 SaaS におけるインシデント対応の責任と手順

業界内でもしばしば誤解されますが、デジタル情報資産をクラウドに移行しても、（マネージドサービス契約において明示的な契約上の合意があれば、例外もあり得ますが）責任や説明責任が完全に移転することはありません。最終的に、資産（およびそこに存在するデータ）の所有者が、さらされたリスクに見合った当然の注意を払いながら、それらを管理するすべての責任を負います。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、SaaS モデルは、他のモデル（PaaS と IaaS）と比較して、プロバイダーが最も責任を負うモデルです。CSA's Security Guidance v4 の 20 ページにあるように、SaaS では、クラウドプロバイダーがほぼすべての層のセキュリティに責任を負います。クラウドサービス利用者（Cloud Service Customer; CSC）が管理できるのは、（クライアントデバイスを含む）アプリケーションのアイデンティティとアクセス、アプリケーションが扱う情報の統制、そして、これはプロバイダーによりますが、データの暗号化設定（Bring Your Own Key など）に限られます。CSC は、仮想化、ネットワーク、境界セキュリティを制御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参照してください。

責任	オンプレ	IaaS	PaaS	SaaS	FaaS
データの分類と説明責任	●	●	●	●	●
クライアントとエンドポイントの保護	●	●	●	●●	●●
アイデンティティとアクセスの管理	●	●	●●	●●	●●
アプリケーションレベルの制御	●	●	●●	●●	●●
ネットワーク制御	●	●●	●	●	●
ホストのインフラ	●	●●	●	●	●
物理セキュリティ	●	●	●	●	●

● クラウド利用者の責任　● クラウドプロバイダーの責任　●● 責任の共有

このモデルでは、いくつかの技術的な責任が移転するため、組織のセキュリティ要件や標準的なベースラインに合わせて、明示的な契約上の合意をクラウドサービスプロバイダーと結ぶことが必須です。CSC は、CSA Consensus Assessment Initiative Questionnaire を調達の段階で活用し、この議論をうまく進めることができるかもしれません。前述したとおり、CSC はどのような状況でも、組織の情報と資産を保護する説明責任を負います。責任は移転できますが、説明責任は移転できません。

利用者のインシデント対応計画は、このような技術的制約を組み込むように更新する必要があり、また CSP の重要な連絡先の登録簿を管理しなければなりません。セキュリティおよびセキュリティ以外のインシデントに関するサービスレベル合意書は、契約書によって合意し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、組織が（サイバー）セキュリティの事象にどのように対応するかは、準備状況が直接関係します。SaaS サービスでは、組織の（認可済）SaaS の概観を確実に把握することが不可欠です。すべての SaaS サービスを調達プロセスの中で審査するべきであり、組織のリスク選好、および規制や業界のコンプライアンス要件に合わせた、信頼できるサードパーティーリスク分析を審査に含める必要があります。CSC が直接（技術的に）管理できない範囲で見つかったリスクを評価しなければならず、必要であれば、契約によって軽減しなければなりません。

CSC にとっては、サプライチェーンリスクと事業目標の継続の観点から、（機密性、完全性、可用性を評価して）サービスの重要度を理解することが最優先です。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、全社の一元的な資産データベースに登録し、インシデント対応者（または CSIRT の他のメンバー）に知らせなければなりません。

必要に応じて、SaaS に特化したプレイブックを、このサービスモデルに該当する脅威や不正使用のシナリオに合わせて作成しなければなりません。SaaS プロバイダーが侵害された場合に、組織の（内部および外部の）ステークホルダーに連絡するコミ

ュニケーションのドラフトを準備することができます。影響がまだ明確でない場合や、まだ完全に収束していない場合でも、声明を出して、顧客やパートナーに積極的に通知することができます。各 SaaS サービスのパラメーターやタグを一元的に保管（CMDB など）することは、どのような種類のコミュニケーションを行うべきかを判断する際に役立ちます（例えば、そのテナントが個人の顧客データを管理しているか）。

11.4 フェーズ 2: 検知と分析

CSC が責任を負うのは、データとデータへのアクセスの保護に限られるため、SaaS の文脈におけるインシデントのほとんどが CSP 所有のシステムによって検知されます。しかし、Identity Provider のアラートや通知、SaaS サービスのアクセスログを使って、CSC も不正アクセスを注意深く監視する必要があります。（ハニートークンなどを使った）データ流出や偵察の検知は、CSC がすべての責任を負います。このため、CSC は、すべての SaaS サービスを、多要素認証を含む組織のアイデンティティプラットフォームに統合することを目指さなければなりません。そして、CSP からのアラートを、CSC の標準的なインシデント対応プロセスに組み込むべきです。できれば、アラートの取り込みと、ビジネスに対する SaaS サービスの重要度を反映した、適切な優先度の割り当てを自動化します。CSP がサポートする場合、CSC の SIEM や IDS ソリューションにログを取り出すべきです。

上記の内容に関わらず、SaaS の CSP のステークホルダーと締結した契約を活用することが不可欠であり、契約に含まれる合意済のサイバー条項を行使して、機密性、完全性、可用性に関する潜在的な侵害を分析するために必要なサポートを得ます。最後に、フォレンジック調査には、CSP の関与が必須です。

11.5 フェーズ 3: 封じ込め、根絶、復旧

ここまでのフェーズと同様に、CSC による対応には制限があります。CSC ができることは、発信元 IP アドレスにもとづくテナントへのアクセス制限（いわゆる許可リストですが、未対応の SaaS プロバイダーもあります）、ユーザーやアカウントのアクセス権限の失効（OAuth による認可、鍵のローテーション、多要素トークンなどを含む）、保存中のデータの暗号鍵のローテーションなどに限られます。

復旧に関しては、CSC のデータバックアップと復旧の計画を発動させるために、CSP に必要なサポートを依頼することが不可欠です。CSC がサードパーティーのバックアップツールを使ったり、CSP にテナントデータのリストアを依頼したりして進めます。

11.6 フェーズ 4: インシデント後の対応

深刻な危機を決して無駄にしてはいけません。少し立ち止まって、学んだ教訓をレビューすることは、堅実なインシデント対応プロセスの極めて重要な最後のステップです。インシデントをレビューし、計画のどの要素が改善できるか見極めます。技術的なものもあれば、管理的なもの（SaaS プロバイダーとの契約上の合意の漏れや、プロセスにおける手順の漏れなど）もあります。主な質問には、以下のようなものがあります。

- 時間通りにイベントを検知できましたか。それとも改善できますか。(メトリクスやログ)
- ベンダーから必要なサポートを得られましたか。(契約や SLA)
- 定められた時間内にステークホルダーに通知できましたか。（コンプライアンスとコミュニケーション）

この行動後の報告書の内容は、学んだ教訓としてフェーズ 1 に直接フィードバックされ、CSC が（SaaS の）インシデントをより良く管理するための準備に役立てるべきです。インシデント後の分析は、ただ時系列やイベントを整理するだけでなく、学びの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、元々、Jeli、Netflix、Slack、Adaptive Capacity Labs が共著した「how we got here」、すなわち、「howie」のプロセスがあります。

他にも、このようなインシデント後の情報が、同業者や他 CSP の役に立つかを評価しなければいけません。ステークホルダーに向けてメッセージを公表したり（例えば、2021 年 11 月 16 日の Google Cloud の障害）、CSA の Cloud Cyber Incident Sharing Center（CloudCISC）を活用したりする選択肢があります。CSA の Cloud Incident Response Framework の第 6 章を、情報共有や調整の指針として参照してください。

12. コンプライアンス

12.1 セキュリティポリシーや標準への準拠

機微なデータを保存し、処理する SaaS アプリケーションは、他のすべての組織のシステムと同じ方法かつ同じ厳しさで、社内外の関連するすべてのコンプライアンス標準やセキュリティポリシーに対して評価しなければなりません。特に、SaaS アプリケーションは、取り扱うデータの種類と秘密度に加えて、リスクにさらされるレコード数、組織の依存度、継続性などの関連するリスク要因を考慮して、カテゴリーに分類し、評価するべきです。

少なくとも、組織はコンプライアンスのため、以下を理解し、文書化し、監視しなければなりません'。

- SaaS アプリケーション内のデータに関連する分類
- SaaS アプリケーションの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で、それぞれの種類のユーザーがどの分類のデータにアクセスできるか
- SaaS アプリケーション内に実装しているアクセス制御
- SaaS アプリケーションが提供する監査機能
- SaaS 利用者に関連する、適用可能なコンプライアンスフレームワークに対するアセスメントや認証

特に、機微なデータやコンプライアンスに関連するデータを含み、かつ外部のユーザー（従業員以外の一般ユーザー）にポータルなどの入り口を公開している SaaS アプリケーションは注意が必要です。これらの SaaS アプリケーションは、構成を誤るとコンプライアンス要件から大きく逸脱する可能性があるため、特に慎重な精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につながります。

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、四半期または年 1 回など、必要に応じて行ないますが、セキュリティとコンプライアンスの両方の要求事項を満たすことができる自動化された継続的な監視システムを導入することがより効果的です。継続的な監視システムを構築するための労力は、一般的に、コンプライアンス評価サイクルの 1 回において、コンプライアンスを検証するために必要な労力と同等です。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評価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逸脱してい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、従来の特定時点のスナップショットに対するアセスメントではなく、準リアルタイムのコンプライアンスを保証することができます。

継続的なモニタリングソリューションの導入には、一般的に以下が必要です。

- 各コンプライアンスフレームワークに関連し、対象となる SaaS アプリケーションを特定します。
- 関連する各 SaaS アプリケーションにおいて、どのユーザーグループが対象となり、にコンプライアンスの懸念があるかを特定します。
- 関連するコンプライアンスフレームワークの要求に必要な 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対応付けます。
- SaaS アプリケーションのアクティビティに対して、自動化された継続的な監視およびレポートを行うため、ソフトウェアベースのツールを活用します。

これらの取り組みが完了し、継続的な監視ソリューションが導入されると、SaaS アプリケーションとそのデータが、関連するすべての組織内の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の確認が、ほぼ自動化されたプロセスになります。継続的な監視を利用すると、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、および特定の期間、コンプライアンスに準拠していたことを検証するための成果物を、必要なときに作成することができます。

独自のデータ保持期間を要求する場合、契約段階での交渉が最善です。独自の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、その処理に使用したデータが SaaS ソリューションから永久に削除されるのはいつでしょうか。SaaS ソリューションにデータ保持の法的義務がある場合、一定の間隔で、処理済のデータをオフラインストレージに移動させることができますでしょうか。独自のデータ保持期間を要求することで、大幅にリスクを低減できます。

12.2 法令や契約からの要件の遵守

12.2.1 適用される法令や契約からの要件の特定

「10. サプライヤーとの関係」の「10.1.2 サプライヤーとの契約で行うセキュリティ対応」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 が利用者のデータにアクセスする権利を留保することがあります。CSP は、特定業務について、サードパーティーのベンダーと契約することがあります。その結果、外部の企業がクラウド利用者のデータにアクセスする可能性があります。

12.3 情報セキュリティのレビュー

上述した継続的な監視ツールや運用を活用することで、組織の SaaS 利用に対する情報セキュリティレビューを容易にすることができます。このレビューには、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への準拠、十分なセキュリティ衛生の実現などを含みます。情報セキュリティレビューには、組織の SaaS 管理台帳の評価や、認可されていない可能性のある SaaS 利用の特定も含めるべきです。

13. CASB の機能と今後の展望

Cloud Security Access Broker の分野は、SaaS サービスの普及にともない注目を集める重要な分野のひとつであり、可視化、監視、シャドーIT（組織の IT 部門が認可しておらず、セキュリティが確保されていないサービス）の制御に焦点を当てています。これらには、以下の主要な機能を含みます。

- リスクについての洞察：初期のユースケースは、利用者が提供する組織外向けの通信ログを、個々のクラウドサービスに関する独自のリスクデータとともに分析し、次のような洞察を提供することでした。
  - 利用者の環境で使われてい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（リモートデスクトップ制御、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ー）
  - 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
  - 組織のクレジットカードを利用して取得したクラウドサブスクリプションのうち、認可を得ずに購入したアプリケーション

この可視化の結果は、ビジネスの意思決定者にとって予期せぬものでした。次に問われる質問は、もちろん、見えるようになったリスクの制御についてでした。

- API：この方式は、API を活用して、追加の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、大量のデータ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、組織の特定のデータに対する外部組織からのアクセスを削除することなどが挙げられます。この方式では、ポリシーに対して行うすべてアクションが、準リアルタイムです。
- インライン：この方式は、最も包括的な対応を提供します。実際に、アプリケーションの通信を CASB クラウドに迂回させ、通信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、従来の許可や禁止のポリシーの代わりに、より細かいポリシーを適用します。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あります。

もうひとつの注目を集める分野は、SaaS Security Posture Management（SSPM）です。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、CIS や NIST などの業界標準に対応付けて事前定義されたポリシープロファイルと比較して、SaaS アプリケーションを継続的に監視します。構成ミスはすぐに通知され、悪用される前に問題を自動的に修正することもできます。

これらの分野は進化を続け、Secure Services Edge（SSE）という新しい分野に収斂されています。この進化の分析は本書の範囲外ですが、クラウドや SaaS のセキュリティ担当者は継続的に追跡するべきです。

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。この加速にともない、組織がクラウドサービスを運用および利用する方法に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 のニュアンスは、さらなる注意と対処を必要とします。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慮が極めて重要になります。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、プロバイダーから 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ー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プラクティスは、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、組織がオペレーションの方法を変更し、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がや予期せぬ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

Cloud access security brokers (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ーの間に設置される、オンプレミスまたはクラウドベースのセキュリティ実施ポイントです。クラウドベースのリソースにアクセスする際に、組織のセキュリティポリシーを挿入します。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、SSO、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、ログ出力、アラート、マルウェア検知と防止などがあります。[6]

Software as a Service (SaaS):クラウドインフラで動作するプロバイダーのアプリケーションを使うための機能を利用者に提供します。アプリケーションは、さまざまなクライアント端末から、Web ブラウザなどのシンクライアントインターフェース（Web ベースの電子メールなど）や、プログラムインターフェース経由でアクセスします。利用者は、ネットワーク、サーバー、おオペレーティングシステム、ストレージ、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または制御しません。ただし、一部のユーザー固有のアプリケーション設定は例外となる場合があります。[7]

Software Bill of Materials (SBOM): ソフトウェアを構築するために使用する、さまざま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ます。[8]

SaaS Security Posture Management (SSPM): Slack、Salesforce、Microsoft 365 などのクラウドベースの SaaS アプリケーションに対する自動化された継続的な監視を提供し、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 チームによるコンプライアンスの確保を支援します。

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。機能には、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、および、ネットワークベースまたは API ベースの統合による許容可能な利用の制御を含みます。SSE は、主にクラウドベースのサービスとして提供され、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。

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

[7] https://csrc.nist.gov/glossary/term/software_as_a_service

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

17. 略語

AICPA - American Institute of Certified Public Accountants（米国公認会計士協会）

API - Application Interface

CASB - Cloud Access Security Broker

CIA - Confidentiality, Integrity, Availability（機密性、完全性、可用性）

CCM - Cloud Control Matrix

CSA CCM - Cloud Security Alliance Cloud Control Matrix

CSA STAR - Cloud Security Alliance Security, Trust, Assurance, and Risk

CSC - Cloud Service Customer

CSP - Cloud Service Provider

DLP - Data Loss Prevention

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 - International Electrotechnical Commission（国際電気標準会議）

ISMS - Information Security Management System

ISO - International Organization for Standardization（国際標準化機構）

NIST - National Institute of Standards and Technology（国立標準技術研究所）

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

OTP - One-Time Password

PaaS - Platform as a Service

PCI - Payment Card Industry

PII - Personal Identifiable Information（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（ソフトウェア部品表）

SIEM - Security Information and Event Management

SLA - Service-Level Agreement（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 - Virtual Machine（仮想マシン）

ZTNA - Zero Trust Network Architecture