スタートアップのための
クラウドセキュリティ
2024

CSAJC cloud security alliance℠ Japan Chapter

CSA cloud security alliance®

About the CSA Israel Chapter

この文書は、Cloud Security Alliance（CSA）のイスラエル支部によって作成されました。CSA イスラエルチャプターは、イスラエル市場における責任あるクラウド導入の推進に尽力するセキュリティ専門家のグループによって設立されました。彼らの使命は、イスラエルの革新的な技術シーンに価値ある知識とグローバルなベストプラクティスを提供することです。詳細と会話への参加については、フェイスブックのグループをご覧ください。

CSAイスラエルの過去の出版物

Cloud Security For Startups ver.1 (2017)
The 12 Most Critical Risks for Serverless Applications (2019)
Security Guidelines for Providing and Consuming APIs (2021)
Understanding Cloud Attack Vectors (2023)

Acknowledgments

Lead Authors

Oz Avenstein
Tony Daskalo
Gidi Farkash
Moshe Ferber
Tzach
Horowitz

Contributors

Daniel Begimher
Brit Ben Amitai
Inbar Ben Tsion
Joss Bernstein
Eyal Estrin
Rivky Hoffnung
Alon Kendler
Reut Menashe
Yaniv Menasherov
Oren Motola
Michael Roza
Eitan Satmary
Tani Shapira
Alex Sherman
Omer Taran
Oren Yeger
Koby Zvirsh

Reviewers

Perry-Bright
Sahil Dhir
Rob Doyon
Govindarajan
Lakshmi Gudimella
Rahul Kalva
Ravi Kiran Nizampatnam
Ravi Kumar
Lakshmikanthan
Akhil Mittal
Venkata Naga
Ratnangi Nirak
Ross Nicholas Oneil Thomas
Meghana Parwate
Srija Reddy Allam
Rodrigo Sampaio
Gene Schank
Sreejith Sreekandan Nair
Karthik Venkatesh Ratnam
Junior Williams

CSA Global Staff

Claire Lehnert
Stephen
Lumpe

日本語版提供に際しての告知及び注意事項

本書「スタートアップのためのクラウドセキュリティ 2024」は、Cloud Security Alliance (CSA)が公開している「Cloud Security for Startups 2024」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
2025年02月03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

「スタートアップのためのクラウドセキュリティ 2024」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
高橋　久緒
松浦　一郎, CISSP, CISM, CDPSE
満田　淳
諸角　昌宏

目次

1. はじめに

1.1 モチベーション

クラウド環境は、ほとんどのSaaS（Software-as-a-Service）ベースのスタートアップ企業にとって基盤となるインフラストラクチャとなっています。既存のクラウドセキュリティガイドラインは貴重な洞察を提供しますが、SaaSベースのスタートアップ企業は、カスタマイズされたアプローチを必要とする明確な課題に直面しています。このような企業は、小規模なチームと限られた予算でスタートすることが多いのですが、顧客や利害関係者のセキュリティを確保しながら、短期間で規模を拡大し、エンタープライズとしての完全な成熟度を達成することが期待されています。このような急成長には、エラーの可能性を最小限に抑えたうえで、革新性、スピード、業務効率、および強固なセキュリティ対策による顧客の信頼維持の間で、微妙なバランスを取ることが必要です。

このようなユニークな特性を認識することで、スタートアップ企業には、成熟プロセスを成長・発展段階に沿ったフェーズに分解した専門的なセキュリティガイドラインが必要であることが明らかです。2017年、Cloud Security Alliance（CSA）のイスラエル支部は、これらのニーズに対応するために設計されたこの文書の最初のバージョンをリリースし、数多くのスタートアップ企業の成熟に向けて前進を支援しました。

このたび、特にSaaSベースのスタートアップ企業に焦点を当てた、より包括的なバージョンがリリースされました。この最新ガイドは、企業レベルのセキュリティ成熟度を達成するために必要な戦略的意思決定と戦術的推奨事項を重視しています。また、スタートアップ企業の資金調達ラウンドの非構造的な性質や、急速に成長する企業の進化する能力についても考察しています。

1.2 SaaS ベースのスタートアップとは？

SaaSベースのスタートアップ企業とは、クラウドを活用してインターネット上でSaaSを提供し、互換性の課題や高価なライセンスといった従来のソフトウェアの制限を克服する、若く成長中の企業のことです。インストールが必要な従来のソフトウェアとは異なり、SaaS製品はクラウド上でホストされ、ウェブブラウザからシームレスにアクセスできます。SaaSスタートアップ企業の特徴は、革新的なアプローチ、急成長へのフォーカス、および業務効率性です。

主要な側面

1. コアビジネスモデル
    a. **クラウドベースのデリバリー**：SaaSベースのスタートアップ企業はインターネット経由でソフトウェアアプリケーションを提供するため、ローカル・インストールや継続的なメンテナンスが不要です。
    b. **サブスクリプションモデル**：通常、月額または年額の継続課金により収益が発生するため、ユーザーに柔軟性と費用対効果を提供します。

2. 運用特性
    a. **イノベーションフォーカス**：SaaSベースのスタートアップ企業は、市場のニーズに対応し、既存のプレイヤーを破壊するために、新しいソリューションを開発し、既存のソリューションを改善することで成功を収めています。
    b. **敏捷性と適応性**：ダイナミックな環境で事業を展開するこれらの企業は、俊敏で市場からのフィードバックに基づいて戦略を調整することができ、迅速に反復することができます。
    c. **リーンオペレーション**：効率は非常に重要です。SaaSベースのスタートアップ企業は、最小限のオーバーヘッドで価値を提供し、競争力を維持するためにリソースを最適化することに重点を置いています。
3. 成長戦略
    a. **ユーザーの獲得**：大規模なユーザーベースの構築は不可欠です。これには、魅力的な機能と卓越したユーザー体験を提供し、コンテンツマーケティング、パートナーシップ、およびフリーミアムモデルなどのさまざまな戦略を活用することが含まれます。
    b. **市場への浸透**：市場シェアの獲得は極めて重要な目標です。SaaSベースのスタートアップ企業は、月間アクティブユーザー数、コンバージョン率、新市場への拡大の可能性などの指標を重視し、主要なソリューションになるために熾烈な競争を繰り広げています。
4. SaaSの利点
    a. **手頃な価格**：クラウドインフラストラクチャーは、費用対効果の高い配信を可能にし、SaaSソリューションをあらゆる規模の企業が従量課金オプションで利用できるようにします。
    b. **使いやすさ:** SaaSプラットフォームは、直感的なインターフェースと最小限のセットアップ要件により、ユーザーエクスペリエンスを優先します。
    c. **スケーラビリティ**：SaaSインフラストラクチャは、ユーザーの増加に合わせて容易に拡張でき、小規模チームから大企業まで効率的に対応します。

本書が他のクラウドセキュリティガイドと最も大きく異なる点は、SaaSベースのスタートアップ企業特有の成長軌道に合わせてセキュリティに関する推奨事項を調整している点です。一般的なクラウドセキュリティガイドとは異なり、規模が拡大するにつれて進化するビジネスのニーズに対応します。

1.3 スタートアップフェーズ

セキュリティの面では、SaaSベースのスタートアップ企業は通常、明確な段階を経て進歩します：創業、成熟、成長。各フェーズでは、スタートアップ企業の開発段階に特有の課題と機会に対応します。

初期段階-フェーズ1（プレシードからシリーズA）では、小規模なチーム、初期の顧客ベース、限られたセキュリティ予算を考慮します。後々コストのかかる失策を避けるため、強固なセキュリティ基盤を確立することに重点を置いています。それはセキュリティの要点を効率的に行うことです。

成熟期-フェーズ2（ラウンドA/シードからラウンドB）では、スタートアップ企業は成熟し、成長しています。従業員も増え、顧客基盤も拡大しているため、セキュリティに対する要求も高まっていきます。セキュリティは成熟し、一般企業に似てきます。

成長段階-フェーズ3（シリーズB終了後）、スタートアップ企業のセキュリティ予算が整っていること。この会社は成熟しており、何百人もの従業員と顧客を抱えています。セキュリティコントロールは成熟しており、規制の厳しい業界でも十分なはずです。

本書の各章では、これらのフェーズに合わせた提言を行っています。しかし、これらの提案を、ご自身のスタートアップ企業の具体的なリスクと能力に照らして検証することが重要です。

SaaSベースのスタートアップ企業の中には、以下のようないくつかの要因によって、より迅速にフェーズを進める必要がある場合もあります。

- **ターゲットマーケット**：特に金融、ヘルスケア、政府、および国土安全保障など、規制の厳しい分野の企業向けのスタートアップ企業は、より厳しいセキュリティ要求と成熟の加速に直面することがよくあります。
- **データ量と感度**：個人を特定できる情報（PII）を大量に扱うスタートアップ企業や、健康記録や財務記録のような機密性の高いPIIを扱うスタートアップ企業は、特定の規制が必要であり、ゲームの早い段階でデータセキュリティコントロールを追加する可能性があります。
- **クリティカルアクセス**：顧客の重要なインフラストラクチャ、アプリケーション、およびデータにアクセスするスタートアップ企業で、運用の完全性を保護するためにセキュリティが最も重要な場合（顧客の重要なアプリケーションにエージェントを配置するアプリケーション監視のSaaSスタートアップ企業など）。

- **マーケティングの優位性**：競争上の差別化要因として堅牢なセキュリティコントロールを導入することで、市場での地位強化を目指すスタートアップ企業。

2. クラウドプラットフォーム

2.1 適切なプロバイダーの選択

ほとんどのSaaSベースのスタートアップ企業は、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP)などのハイパースケールのパブリックIaaS/PaaSプロバイダーを基盤としてベンチャーを立ち上げます。これらのベンダーは、エンタープライズグレードのアプリケーションを作成し、迅速にデプロイするためのインフラストラクチャと開発ツールをスタートアップ企業に提供しています。プロバイダーを選択する際、スタートアップ企業はセキュリティとコンプライアンスの要件を考慮する必要があります。

さらに、パブリッククラウドプロバイダーがセキュリティの推奨事項の特定の側面を処理するため、スタートアップ企業はこの領域で成熟度を示すことが容易になります。

2.2 SaaS、IaaS、PaaS 用語

米国国立標準技術研究所（NIST）のクラウド定義によると、クラウドサービスは3つのサービスモデルに分類されます：IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）。

IaaSでは、スタートアップ企業が仮想マシンのオペレーティングシステムのパッチ適用、スケーリング、およびセキュリティ設定を管理します。PaaSを利用することで、スタートアップ企業は、アプリケーションの設定やセキュリティの管理には責任を負うものの、基盤となるインフラストラクチャ（オペレーティングシステム（OS）のメンテナンスなど）の心配をすることなく、アプリケーションの開発に専念することができます。その結果、PaaSの領域では、スタートアップ企業はプロバイダーのインフラストラクチャ仕様の一般的な枠組みに準拠するようにアプリケーションを修正し、オペレーティングシステムの基礎レイヤーの管理から免れるというメリットを享受しています。顧客はOSの管理から解放されたとはいえ、可用性の高いアーキテクチャでインフラストラクチャのコンピュートノードをプロビジョニングする責任は残っていることに注意が重要です。クラウドネイティブ企業は、開発と保守を合理化するために、サービスの大部分をPaaS上に構築することがよくあります。しかし、PaaSが理想的な選択ではない場合もあります。スタートアップ企業は、カスタム設定が必要な場合、サービスクォータに制限がある場合、またはPaaSプラットフォームが提供しない機能が必要な場合に、PaaSから移行する必要があります。

スタートアップ企業は、著名なIaaS/PaaSプロバイダーで開発の旅を始めるべきです。その後、顧客の要望に応えたり、新たな市場を開拓するために、IaaS/PaaSプラットフォームで存在感を示すかもしれません。この章では、これらのサービスタイプのセキュリティ確保に焦点を当てます。

スタートアップ企業は、業務のさまざまな分野にまたがって、さまざまなSaaSソリューションを利用することができます。これらのサービスには、コードリポジトリ、チケット、および変更管理などのアプリケーションに直接関連するサービス、分散型サービス拒否（DDoS）攻撃防御などのセキュリティサービス、電子メールや文書管理、アイデンティティプロバイダー、会議室、および電話などの広範な情報技術（IT）サービスが含まれます。

SaaSプロバイダーは、すべてのスタートアップ企業のセキュリティスタンスを形成する上で重要な役割を果たしています。顧客は、サードパーティやサプライチェーンのリスク管理の一環として、こうしたプロバイダーの身元を広く照会し、セキュリティ能力やポスチャを評価することがよくあります。この文脈での重要なアドバイスは、スタートアップ企業が顧客のデプロイメント後期にセキュリティ上の障害とならないよう、SaaSプロバイダーを慎重に選択することです。スタートアップ企業が進化するにつれて、サードパーティサービスのセキュリティ確保が重要になってきますが、このトピックについては「ガバナンス、リスク、コンプライアンス」の章でさらに詳しく説明します。

2.3 責任の共有について

責任共有モデルはクラウドコンピューティングの基本概念です。クラウドサービスプロバイダーとその利用者が協力し、セキュアで適切に管理されたクラウド環境の確保を重視します。このモデルでは、クラウドプロバイダーと利用者の間でセキュリティと運用タスクの責任が分散されます。プロバイダーは、物理データセンター、ネットワーク、ハイパーバイザーなどのクラウドインフラストラクチャーのセキュリティを管理します。一方、「クラウド内」のデータのセキュリティ確保、アクセス制御の管理、セキュリティ構成の設定、およびクラウドサービスの適切な利用の確保は利用者の責任です。

ほとんどの場合、責任共有モデルは、SaaSからPaaS、IaaSへと移行するにつれて、クラウドサービスプロバイダーから利用者へと段階的に責任が移行していくことを表しています。SaaSベースのスタートアップ企業の場合でも、特定の重要な責任は顧客（SaaSベースのスタートアップ企業）に残ることを強調します。これには、顧客データ、インターフェース、アイデンティティ管理、および監査プロセスの管理と保護が含まれます。

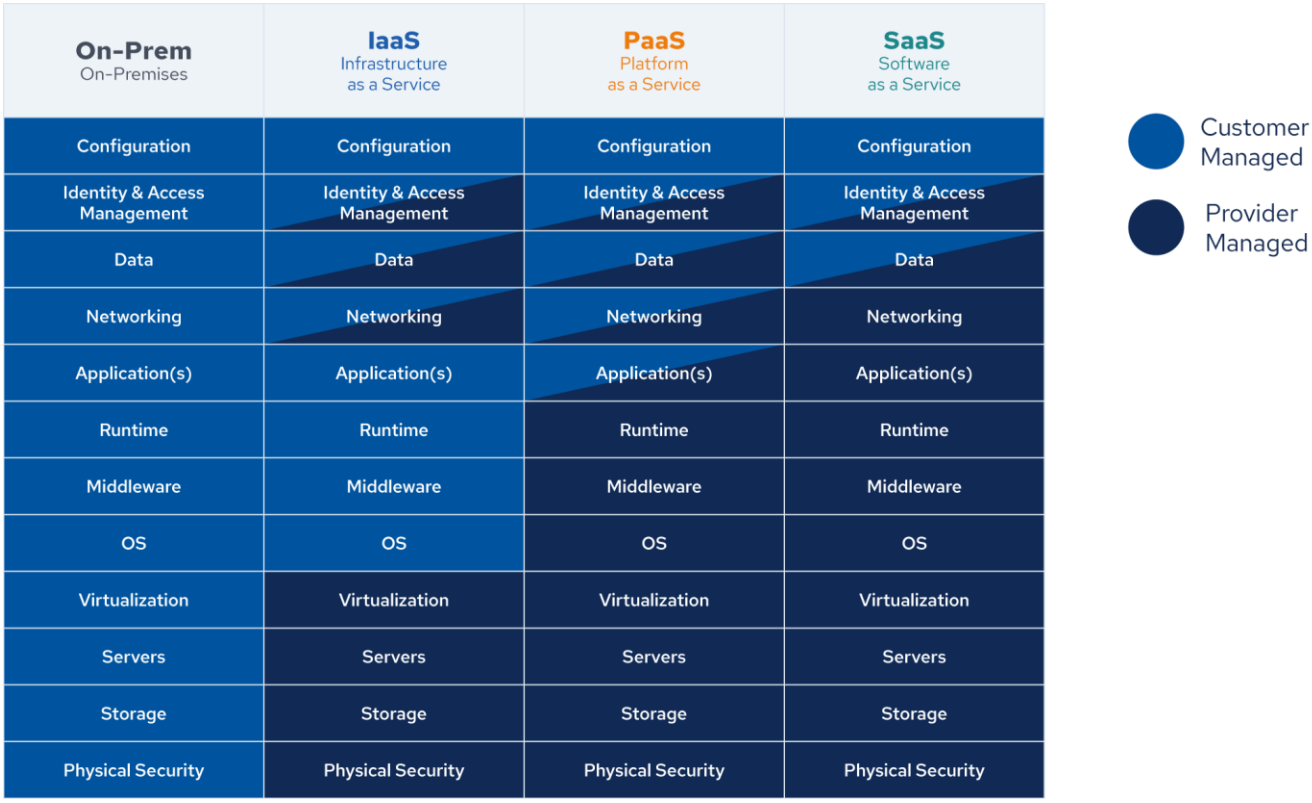


図1: セキュリティ責任共有モデル

24 クラウドデプロイメントモデル

NISTのクラウド定義によると、クラウドコンピューティングには4つのデプロイメントモデルがあります：プライベート、パブリック、ハイブリッド、コミュニティ。SaaSベースのスタートアップ企業に関しては、そのほとんどがパブリッククラウドサービス上に配備されていると断言するのが一般的に正確です。これらのスタートアップ企業は、パブリッククラウドサービスのポートフォリオを構築し、利用者に提供するために、パブリッククラウドサービスに依存することがよくあります。

米国政府のクラウドのように、プライベートクラウドを提供するスタートアップ企業もあります。しかし、これは通常、主要な公共サービスに追加する形で提供されています。

クラウドデプロイメントの詳細については、CSA ガイダンス v.5、ドメイン 1、セクション 1.2.3 を参照してください。

2.5 クラウドプラットフォームの選択

2.5.1 要件を理解する

セキュリティ要件は市場分野によって異なり、収集するデータの種類に大きく依存します。すべての規制、ベストプラクティス、および標準の約90%が同じです。しかし、機密性の高いデータや規制の厳しい市場分野では、より迅速な成熟度と管理体制の精査が求められます。

スタートアップ企業のロードマップを計画する際、ベンダーは、どの時点でどのセキュリティコントロールを組み込む必要があるかを見積もり、計画を立てる必要があります。スタートアップ企業の特徴が以下のいずれかに当てはまる場合は、早期にセキュリティコントロールを実施する準備が必要です。

- 対象となる顧客が企業の場合、責任共有モデル、アイデンティティ管理、およびセキュリティポリシーに関する質問の増加が予想されます。
- 収集/保存されたデータに大量の個人識別情報（PII）や機微なPII（健康情報や財務情報など）が含まれる場合、 Health Insurance Portability and Accountability Act (HIPAA)、一般データ保護規則(GDPR), ペイメントカード業界データセキュリティ基準(PCI DSS)など、より厳格な規制や法律に準拠する必要がある場合があります。
- 対象分野が医療や金融の場合、業界特有の規制やデータセキュリティに関する質問の増加が予想されます。
- 政府、軍事、防衛、および兵器産業をターゲットにしている場合は、データの場所やプライベートクラウド（AWS GovCloud、UK MOD Cloudなど）の使用に関する要件が予想されます。

2.5.2 市場における代替品

SaaSベースのスタートアップ企業は、ハイパースケールクラウドプロバイダー（グローバルなインフラストラクチャ、大規模なスケーラビリティ、大企業やスタートアップ企業にも対応する高度なサービスを提供するクラウドプロバイダー）のいずれかをビジネスに選ぶべきです。定評のある成熟したクラウドプロバイダーを利用することで、将来的な複数地域への拡大や、将来的な成熟に必要な標準やベストプラクティスの遵守に対する基本的なサポートを確保し、顧客を安心させることができます。

ハイパースケールクラウドプロバイダーの標準的な定義はありません。それでも、一般的には以下のようなメリットがあると考えられています。

- **グローバルリーチ**：ハイパースケールプロバイダーはグローバルにデータセンターを展開しており、低遅延、災害復旧、および地域間の規制遵守を保証しています。
- **スケーラビリティ**：ハイパースケーラは、VM、ストレージ、およびデータベースなどのコンピューティングリソースのオンデマンドスケーリング機能を提供します。これらの機能により、ユーザーはコストを最適化し、需要に対応し、成長をサポートできます。
- **先進技術**：ハイパースケールクラウドプロバイダーは、基本的なコンピュートやストレージの提供にとどまらず、人工知能（AI）や機械学習（ML）、ビッグデータ分析、モノのインターネット（IoT）、マイクロサービスアーキテクチャ、コンテナ化など、先進的なサービスを包括的に提供しています。
- **高い可用性と信頼性**：ハイパースケーラは、アップタイムを優先し、 冗長システム、災害復旧計画、サービスレベルアグリーメント（SLA）のサポートなど、サービスの継続性を確保するための対策を実施します。
- **セキュリティ**：ハイパースケーラは、顧客のデータとアプリケーションを保護するために、堅牢なセキュリティ対策を優先します：セキュリティ・アット・スケール、セキュリティ自動化、専門知識への投資、およびコンプライアンス認証。
- **プライバシー**：ハイパースケールクラウドプロバイダーは、 データ匿名化・仮名化、データ暗号化、データ常駐オプション、アクセスログ、およびモニタリングなど、ユーザーのデータプライバシー管理に役立つ機能やサービスを提供するようになってきています。

IaaS/PaaSプロバイダーを選択する際のその他の考慮事項は以下の通りです。

- **データレジデンシー**：特定の地理的管轄区域の企業をターゲットとする場合、データ主権を維持することが推奨されます。そうすることで、コンプライアンスの達成を支援し、競争上の優位性を生み出すことができます。
- **規制**：クライアントは、同じ規制体制に沿ったサービスプロバイダーと協力するよう努めなければなりません。
- **エコシステム**：スタートアップ企業は通常、開発時間を短縮するために外部のソフトウェアやサービスを利用しようとします。知識、ツール、およびサードパーティソフトウェアの大規模なエコシステムは、クラウドプロバイダーにとって有利です。
- **スタートアップ企業への特典**：ほとんどのクラウドプロバイダーは、新しいスタートアップ企業に対し、資金バウチャーや割引、専門家による支援、マーケティングやネットワーキングの促進など、さまざまな特典を提供します。

2.5.3 所在地

GDPRやCalifornia Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA)のようなプライバシー法は、データレジデンシー要件の重要な推進要因ですが、それだけが要因ではありません。政府機関や規制の厳しい業界をターゲットとするスタートアップ企業は、プライバシーの心配だけでなく、特定の政府方針によるデータレジデンシーの追加要件に遭遇する可能性があります。データレジデンシーの

要件が広まるにつれ、スタートアップ企業は、新しい地域に進出する際にコンプライアンスを確保できるよう適応しなければなりません。

第4章「セキュリティ管理-プライバシーの考慮事項」では、プライバシー法およびデータレジデンシーの考慮事項に関する詳細情報を提供しています。（訳注：原書では「Chapter 4, Security Management—Privacy Considerations」となっていますが、「4.2 クラウドセキュリティにおけるプライバシーとデータ保護の考慮点」の間違いと思われます）。

25.4 マルチクラウドの考察（IaaS/PaaS）

マルチクラウドのデプロイメントには高度な成熟度と自動化が必要であり、SaaSベースのスタートアップ企業にはこのアプローチを取る十分な理由があるはずです。マルチクラウド化の理由としては、以下のようなものが考えられます。

- **可用性と冗長性**：スタートアップ企業は、可用性に依存して、1つのプロバイダーがダウンした場合のリスクを軽減するために、2つの異なるクラウドプロバイダーを使用できます。
- **顧客の要件**：顧客によっては、スタートアップ企業とは異なるクラウドプラットフォームを必要とする場合があります。これは、スタートアップ企業のセキュリティポスチャに影響を与えるビジネス上の決断です。
- **新しい地域をカバー**：スタートアップ企業の中には、中国市場向けの現地プロバイダーなど、場所によって異なるプロバイダーを利用するところもあります。

マルチクラウド化を進めるSaaSベースのスタートアップ企業は、以下のような課題に直面することになります。

- **複雑さの増大**：インターフェース、アプリケーションプログラミングインターフェース（API）、および課金構造を持つ複数のクラウドプラットフォームを管理することは重要です。混乱を避けるためには、熟練した運用チーム（DevOps）と堅牢な自動化ツールが必要です。
- **アイデンティティとアクセス管理（IAM）**：オンボーディング、オフボーディング、およびユーザーアクセス管理は、複数のクレデンシャルとポリシーを扱うと複雑になります。
- **セキュリティ上の懸念**：データとアプリケーションを複数のクラウドに分散させると、潜在的なセキュリティ侵害のアタックサーフェスが広がります。異なるプラットフォーム間で一貫したセキュリティポリシーを維持することは困難な可能性があります。
- **ベンダーロックイン**：マルチクラウドは単一のベンダーへの依存を避けることができますが、複雑な移行を伴う複数のクラウドプロバイダーの管理に伴うトレードオフも同様に問題となります。
- **コスト管理**：さまざまな料金体系を持つクラウドプロバイダー間でコストを追跡することは困難な可能性があります。クラウドスプロールのリスクがあり、未使用のリソースにお金を払うことになります。
- **人材不足**：複雑なマルチクラウド環境を管理できる専門知識を持ったITプロフェッショナルを見つけることは、特にリソースが限られているスタートアップ企業にとっては難しいことです。

- **監査／可観測性**：セキュリティとパフォーマンス監視のために複数のクラウドプロバイダーからログを収集し分析することは、すべてのクラウドプラットフォームのアクティビティとリソース利用を完全に把握することと同様に、問題が生じる可能性があります。
- **コンプライアンスの複雑さ**：地域によって規制が異なるため、一貫したコンプライアンスポスチャーを維持することを難しくします。

2.6 アーキテクチャ

2.6.1 要件の検証

このセクションでは、既知のIaaS/PaaSプロバイダー（AWS、Azure、GCP、OCIなど）に実装されたスタートアップアプリケーションのアーキテクチャに焦点を当てます。私たちは、効果的なアーキテクチャを確実に作成するために、希望するインフラストラクチャの要件を綿密に検証することから始めることをお勧めします。要件は、現在の運用の成熟度に合わせ、潜在的な成長と将来の拡張性を予測する必要があります。例えば、「プラットフォームは、米東部地域の顧客に高いパフォーマンスを提供すること」という要件があります。「グローバル展開を目指すスタートアップ」は、次のようなフレームを持つべきです：「このプラットフォームは、まず米国・東部地域の顧客に高いパフォーマンスを提供し、将来的にはさらなる地域への成長を可能にする。」

要件はできるだけ具体的で、以下の領域をカバーするものでなければなりません。

- **インフラストラクチャとネットワーク**：アプリケーションをサポートするために必要なインフラストラクチャ要素と機能を明確に定義します。
- **IAM**：アイデンティティが管理される場所と、ユーザーアクセスに必要なプロトコル、認証方法、および認可メカニズムを指定します。
- **データ保護とプライバシー**：特に機密情報に関するデータの暗号化、保管、およびコンプライアンス要件の詳細を説明します。
- **脅威管理とモニタリング**：アーキテクチャがどのようにセキュリティ脅威やインシデントの検出、緩和、および対応する方法を概説します。
- **アプリケーションセキュリティとセキュアな開発**：これらに関する詳細については、3章を参照してください。
- **脆弱性管理**：脆弱性をスキャンする頻度と、特定された脆弱性を修正するスケジュールに関するポリシーを定義します。
- **ガバナンスとコンプライアンス**：アーキテクチャが遵守すべき規制基準、ポリシー、およびガバナンス手順を特定します。これについては4.5章で詳しく説明します。
- **レジリエンスと高可用性**：中断のないサービスと迅速な復旧を保証するために必要な冗長性、フェイルオーバーメカニズム、および災害復旧ソリューションのレベルを定義します。

2.6.2 初期アーキテクチャの構築

初期アーキテクチャの構築は、要件の検証に成功した後の論理的な次のステップです。このフェーズでは、ハイレベル設計（High-Level Design：HLD）を作成します。HLDは、システムの構造を概観し、コアインフラストラクチャー、ソフトウェアコンポーネント、およびセキュリティ対策をマクロレベルで特定します。この設計は、ビジネス目標と技術目標の整合に役立ちます。

HLDは、クラウドアーキテクチャのトップレベルのビューを提供し、以下の側面を含む必要があります：

- **インフラストラクチャの要素**：ワークロード、ストレージ、ネットワーク、その他のクラウドサービスなど、ビジネスプロセスのサポートに不可欠な中核インフラストラクチャーコンポーネントを明確に定義します。
- **セキュリティとコンプライアンス**：事前に検証された要件に沿ったセキュリティ対策とコンプライアンスプロトコルを統合します。
- **ビジネスプロセスの実現**：アーキテクチャが実現すべきビジネスプロセスを特定し、優先順位を付けます。アーキテクチャの各要素が、これらのプロセスの効率的な実行にどのように寄与するかを検討します。

26.3 デプロイメントの場所

クラウドソリューションを導入する場所や地域を考慮することは、特に規制や業界固有の要件に準拠するために非常に重要です。

導入に最適なクラウド地域を決定する際には、以下のようなさまざまな要素を考慮することをお勧めします。

- **規制コンプライアンス**：地域によって、データ保護、プライバシー、およびコンプライアンスに関する規制が異なる場合があります。選択した地域が、顧客のビジネスに関連する法的要件に準拠していることを確認してください。
- **業種別要件**：業種によっては、業種特有の規制や基準によって、特定のクラウドジオロケーションを選択しなければならない場合があります。そのような要件が遵守を確実にします。(政府部門がその代表例）。
- **データレジデンシー**：一部の国や地域には、特定のデータをその地域の地理的境界内に残すことを義務付ける厳しいデータレジデンシー要件があります。これは、政府の要求事項では非常に一般的なことです。
- **サービスの可用性とパフォーマンス:**選択した地域におけるクラウドサービス、サポート、およびリソースの可用性を確認します。サービスの可用性とサードパーティアプリケーションの配備は、地域によって異なる場合があります。
- **多地域展開:**ほとんどのスタートアップ企業は、 市場参入戦略と顧客の所在地に基づいて、単一地域の展開から始めます。事業が成熟し拡大するにつれ、さらに多くの地域や市場にサービスを提供する必要性が高まるでしょう。堅牢なInfrastructure as Code（IaC）プラクティスを実装

することで、新たな地域へのデプロイメントがより合理化され、管理しやすくなります。

26.4 影響範囲の縮小

クラウド環境の影響範囲を小さくすることは、サイバーセキュリティ防御の強化に不可欠です。影響範囲は、データ侵害やシステム侵害などのセキュリティインシデントにおける潜在的な影響と損害の程度を表します。クラウドコンピューティングのダイナミックな状況において、潜在的な影響を制限し、よりレジリエントなセキュリティポスチャを組織に提供します。

影響範囲の縮小を目指すクラウドアーキテクチャを実装する際には、以下の点の考慮をお勧めします。

- **環境の分離**：本番環境、開発環境、テスト環境を明確に分離します。このように分離することで、セキュリティインシデントや違反の影響を抑制し、ある環境での課題が他の環境に連鎖しないようにします。クラウドベンダーによっては、異なるアカウント、サブスクリプション、またはプロジェクトなど、いくつかの方法でこれを実現できます。クラウドプロバイダーにはそれぞれ専門用語があります。
- **イミュータブルなアーキテクチャ**：コンポーネントを変更するのではなく、置き換えるイミュータブル・インフラストラクチャー・アプローチを採用。脆弱性が特定された場合、環境全体をクリーン／パッチ適用済みのバージョンに置き換えることで、露出を制限し、侵害された要素がシステム内に残る時間を短縮することができます。これは、クラウドの変更にInfrastructure as Codeとして組み込むことで実現できます。
- **セグメンテーション**：ネットワークセグメンテーションを導入し、インフラストラクチャのさまざまな部分を分離します。これには、セキュアなゾーンを作り、その間のトラフィックを制御することが含まれます。ネットワークを区分することで、攻撃者のラテラルムーブメントを制限し、潜在的な被害を最小限に抑えることができます。
- **役割ベースのアクセス制御（RBAC）**：最小特権の原則を実施するためのRBACを実装します。これにより、ユーザーとシステムには、タスクの実行に必要な最小限の権限のみが与えられます。ユーザーのアカウントが侵害された場合、そのユーザーのアクセスは制限され、潜在的な損害は制限されます。
- **属性ベースのアクセス制御（ABAC）**は、RBACよりもきめ細かいアクセス制御のアプローチを提供します。ABACでは、役割のみに依存するのではなく、アクセス要求に関わる様々な要素（主体、資源、行為、環境）の属性を考慮し、これらの要素の属性を評価するポリシーに基づいて判断を行います。ベンダーによっては、条件付きアクセスやポリシーベースのアクセス制御という言葉を使います。

助言：セグメンテーションと強力なアクセスコントロールポリシーは、ゼロトラストアーキテクチャを実現するための基盤です。

26.5 ネットワークのセグメント化 - VPC/VNet/サブネット

ネットワークの分離には、クラウドインフラストラクチャー内に個別の隔離されたセグメントを作成し、未認可のラテラルムーブメントを防止し、潜在的なセキュリティインシデントを特定のネットワークゾーンに限定することが含まれます。各クラウドプロバイダーは、セグメンテーションを作成するためのツールを用意しています。AWSとGCPではVPC（Virtual Private Cloud）という言葉を使い、AzureではVNET（Virtual Network）です。

この分離を達成するための主な戦略には、以下のようなものがあります。

- **ハブアンドスポークアーキテクチャー**：このモデルには、さまざまなスポークネットワークに接続する集中型ハブが含まれ、これらのネットワーク間で制御されたトラフィックフローを確保し、出入りするトラフィックに追加のコントロールを行います。
- **集約型ファイアウォール**：集約型ファイアウォールを統合することで、ネットワークセグメント間のトラフィックの検査と制御が可能になります。
- **セグメンテーション**：例えば、クライアント向けワークロード用のセグメントとバックエンド向けワークロード用のセグメントなど、個別のセグメントを作成します。
  別の例としては、各スポークのセグメントがあります。
- **マイクロセグメンテーション**：マイクロセグメンテーションでは、個々のワークロードやアプリケーションの周囲にきめ細かいセキュリティゾーンを作成します（AWSではSecurity Groups、AzureではNetwork security groups、GCPではVPC Service Control Perimeterを実装することで実現できます）。マイクロセグメンテーションは、ハブアンドスポークアーキテクチャーとセグメンテーションの概念をさらに一歩進め、スポーク内部のセグメンテーションに焦点を当てます。マイクロセグメンテーションは、ワークロードをアプリケーションレベルに分離し、ラテラルムーブメントを制限し、アタックサーフェスを減らすことで、ネットワークセキュリティを強化します。

26.6 環境アクセス

ネットワークの分離には、クラウド環境内のさまざまなワークロード（VM、管理対象データベース、コンテナ）へのアクセスを許可するソリューションが必要です。bastionホスト（ジャンプサーバー）は一般的なアプローチです。堀と跳ね橋のような役割を果たし、すべての外部アクセスを単一のセキュアなエントリポイントに通すことで、攻撃者からクラウドリソースを保護します。

以下はなぜ重要なのかを示しています。

- **アタックサーフェスの減少**：侵入口が少なくなり、攻撃が難しくなります。
- **集中アクセス制御**：許可された者だけが跳ね橋を渡ることができ、その動きは監視されています。
- **モニタリングの強化**：警備員（セキュリティシステム）は不審な動きがないか常に監視していま

す。

本来の利点に加え、bastionのコンセプトには次のような利点があります。

- **セキュアなリモートアクセス**：秘密のトンネルのように、このbastionは内部システムへのセキュアなリモート接続方法を提供します。
- **脆弱性管理の簡素化**：すべての壁（個々のサーバー）にパッチを当てるよりも、ゲート（bastion）にパッチを当てる方がアクセス性が良くなります。

今日、クラウドサービスプロバイダー（CSP）やサードパーティは、bastionの必要性を減らし、ゼロトラストのコンセプトに基づくさまざまなアクセスレベルを提供するソリューションを提供しています。AWS System Manager、Azure Just in Time Access、GCP Identity Aware Proxyなどがその例です。これらのサービスは、ゼロトラストの原則に基づき、よりきめ細かなアクセス制御を提供し、必要な場合にのみアクセスを許可し、アタックサーフェスをさらに縮小します。

典型的な最新のスタートアップの実装は、以下のフェーズに従います。

- **フェーズ1:**AWS SSM（System Manager）やAzure Bastionなど、CSPが提供する組み込みサービスを使用して、クラウドリソースへのリモートアクセスを管理し、セキュアにします。
- **フェーズ2:**クラウドリソースへのセキュアかつ一時的なアクセスをサポートするため、パートナーやサードパーティ向けのJITアクセス機能を導入します。これにより、必要なときだけアクセスできるようになり、アタックサーフェスが減少します。
- **フェーズ3:**サードパーティのZTNA（Zero Trust Network Access）ソリューションやPIM（Privileged Identity Management）を導入し、セキュリティをさらに強化します。PIMは特権アカウントの管理とセキュリティ確保に役立ちますが、ZTNAソリューションは、アイデンティティとコンテキストに基づいてアクセスを許可し、従来の境界セキュリティへの依存を軽減します。セキュアアクセスサービスエッジ（SASE）とセキュアウェブゲートウェイ（SWG）ソリューションを導入し、クラウドサービスやその他のSaaS製品へのセキュアでコンプライアンス準拠したアクセスを保証する、ポリシーベースの包括的なセキュリティを提供します。

注：その他の考慮事項については、5.5章を参照してください。

26.7 複数アカウントの論理的分離

本番環境、開発環境、テスト環境など、異なる環境を明確に分離します。このように分離することで、セキュリティインシデントや違反の影響を抑制し、ある環境での課題が他の環境に連鎖しないようにします。

クラウドにおける論理的分離の推奨は以下になります。

- **複数のクラウドアカウントを使用します**：クラウドサービスプロバイダーが提供するマルチアカウント機能を活用します。クラウドのアカウントを個別の環境に割り当てます。アカウント構造と分離は、環境（本番/開発/テスト）、異なる組織単位、異なる顧客、または異なるビジネスアプリケーションに基づいて、強固な分離を確立することができます。
- **組織構造の導入**：AWS組織単位、Azureサブスクリプション、またはGCPフォルダを利用します。この階層構造により、ガバナンスとリソース管理が簡素化されます。
- **集中ポリシーの導入**：ポリシーを使用して、インフラストラクチャ全体を通じて、さまざまなアカウントや組織単位でガバナンスとコンプライアンスを実施します。
    - **AWS:**サービスコントロールポリシー（SCP）を使用して、複数のアカウントの権限を一元管理します。
    - **GCP:**組織ポリシーを活用して、フォルダやプロジェクト全体のセキュリティとリソース管理を標準化します。
    - **Azure:**サブスクリプションレベルでガバナンスとコンプライアンスを実施するためのAzureポリシーを実装します。
- **「共有サービスアカウント」を使用**して、すべてのOUとアカウントで一元化されたサービスを提供します。例えば、ロギングやモニタリング、CI/CDパイプライン、イメージリポジトリなどです。
- **リソースタグの実装**：リソースのタグ付けを利用して、リソースにラベルを付け、環境に応じて分類します。「Environment:Production」、「Owner:IT」、「Project:Security」などのタグを使用して、リソースを分類し、効率的に管理します。これにより、リソース管理とコスト追跡が簡素化され、各環境固有のポリシーの適用が容易になります。
- **環境プロビジョニングの自動化**：Infrastructure-as-Code (IaC) プラクティスを導入し、 環境のプロビジョニングを自動化します。これにより一貫性が確保され、セキュリティの脆弱性につながる設定ミスのリスクが軽減されます。(この文書には、IaCと自動化の使用に関する専用のセクションがあります。このトピックの詳細については、「自動化の使用」のセクションを参照してください)。

2.6.8 ランディングゾーンという言葉の理解

クラウドランディングゾーンとは、ワークロードやアプリケーションをクラウドに配備するための、セキュアで設定済みの出発点です。クラウド環境という荒野に足を踏み入れる前に、必要なものがすべて準備された整然としたキャンプ場のようなものです。

ランディングゾーンを利用すれば、貴重な時間と労力を節約できます。主な例としては、新規顧客のためのリソースの拡大や作成が挙げられます。事前に設定されたテンプレートにより、デプロイメントに対しセキュアな構成がすでに設定されているため、デリバリー時間が短縮されます。

クラウドランディングゾーンを利用するメリットをいくつか紹介します。

- **セキュリティリスクの低減**：ランディングゾーン内でセキュリティのベストプラクティスを実施することで、不正アクセスやデータ侵害のリスクを大幅に減らすことができます。

- **デプロイメントの迅速化**：設定済みの環境を使用すれば、新しいワークロードやアプリケーションをより迅速に導入できます。
- **管理の簡素化**：一元化され標準化されたランディングゾーンによるクラウドリソースの管理はより簡単です。
- **ガバナンスの改善**：明確なポリシーとコントロールにより、規制要件へのコンプライアンスを確保できます。
- **コストの最適化**：ランディングゾーンは、クラウド利用を最適化し、不要なコストの回避に役立ちます。最適化された構成済みのテンプレートを使用することで、ランディングゾーンは過剰なプロビジョニングを防ぎ、不必要なクラウド費用を削減します。
- **スケーラビリティ**：ランディングゾーンはスケーラブルな基盤を提供し、スタートアップの成長に合わせてクラウドインフラストラクチャーを簡単に拡張できます。

ランディングゾーンは、セキュリティオペレーションとコンプライアンスを合理化します。標準的なセキュリティ構成と自動化ワークフローを確立することで、複数のデプロイメントにわたるセキュリティ管理が簡素化され、時間とリソースを節約し、クラウド環境全体で一貫したセキュリティポスチャを維持することができます。さらに、ランディングゾーンは、必要なコントロールと監査証跡を組み込むことによって、HIPAAやPCI-DSSのような特定のコンプライアンス要件を満たすように設計できます。これにより、業界規制の遵守が簡素化され、コンプライアンス違反による罰金や風評被害のリスクが軽減されます。

26.9 自動化の使用（IaC、イミュータブル、テンプレート）

クラウドにおける自動化、特にIaC（Infrastructure as Code）、テンプレート、イミュータブルワークロードによる自動化は、セキュリティ対策の強化に大きく貢献します。

このアプローチを使用することで、次のようなメリットがあります。

- **一貫したセキュリティポリシー**：IaCは、セキュリティポリシーを成文化（*Policy as Code*とも呼ばれる）し、クラウドインフラストラクチャー全体で一貫性のある標準的な構成を確実にします。オープンソースのIaC言語としては、TerraformやPulumiが有名です。
- **バージョン管理された構成**：セキュリティ構成はバージョン管理されているため、各デプロイ前のレビューが容易で、課題が発生した場合は既知のセキュアな状態に簡単にロールバックできます。
- **テンプレートによる迅速なデプロイメント**：テンプレートは、インフラストラクチャーコンポーネントの迅速かつ標準化されたデプロイメントを可能にし、セキュリティ構成の一貫した適用を確実にします。
- **レジリエンス強化のためのイミュータブルなワークロード**：イミュータブルなワークロードは、インスタンス（VM、コンテナ）を変更するのではなく、入れ替えることを容易にし、攻撃者が脆弱性をエクスプロイトすることを困難にし、一貫した、既知の、セキュアな状態を確実にします。
- **アタックサーフェスの減少**：自動化、IaC、テンプレート、およびイミュータブルなワークロード

の組み合わせは、構造化されコントロールされた環境を強制することでアタックサーフェスを減らし、不正アクセスやエクスプロイトを困難にします。

自動化の推奨事項は以下になります。

- **Infrastructure as Code（IaC）の導入**：IaCを採用し、コード形式でインフラストラクチャを定義・管理することで、スタートアップ企業のクラウド配備を開始します。これにより、時間と労力が節約され、インフラストラクチャ構成の一貫性、バージョン管理、および容易な複製が保証されます。
- **成長とともに成熟**：スタートアップ企業が成長し、完成し、成熟するにつれて、IaCの手順はより良いガードレールを備えたより自動的なものになります。これにより、効率が向上し、エラーが減少し、より堅牢なインフラストラクチャ管理が保証されます。
- **セキュリティ強化のためのイミュータブルワークロードの強制**：インスタンスは変更されるのではなく、置き換えられるという、イミュータブルワークロードの概念を取り入れます。このアプローチは、アタックサーフェスを減らし、潜在的な脆弱性がエクスプロイトされにくくし、一貫した既知のセキュアな状態を確保することでセキュリティを強化します。
- **自動化とDevSecOpsの文化を構築**：自動化と開発、セキュリティ、および運用（DevSecOps）の文化を最初から醸成します。開発、運用、およびセキュリティの各チーム間の協力を促し、セキュリティプラクティスを開発パイプラインに統合することで、より迅速でセキュアなリリースを実現します。

これらのプラクティスを早い段階から統合することで、セキュリティが強化され、長期的な運用効率にも貢献します。自動化によって手作業が減り、スタートアップ企業は日常的な保守作業よりもイノベーションやビジネスの成長に集中できるようになります。

初期段階では、スタートアップ企業はクラウドインフラストラクチャーのIaCを完全に自動化して活用するための知識やリソースが不足している可能性があります。したがって、成熟期、特に規模拡大が必要となり顧客基盤が拡大し始める時期に、IaCを導入することを強くお勧めします。この戦略的アプローチにより、スタートアップ企業の進化に伴い、より自動化された効率的なインフラストラクチャ管理システムへのスムーズな移行が可能になります。

26.10 レジリエンスに関する考慮事項の理解

自然災害やサイバー攻撃、および人為的ミスなど、災害にはさまざまな形態があります。スタートアップ企業が災害復旧シナリオを検討すべき時期を認識するには、リスク要因を評価し、そのような計画の妥当性を示すパラメータを確立する必要があります。

災害復旧（DR）シナリオを検討するタイミングは以下になります。

- **重要なビジネス機能**：スタートアップ企業が重要なビジネス機能に依存しており、それが途絶した場合、業務や顧客サービスに大きな影響を及ぼす可能性がある場合は、DRを検討してください。
- **規制の遵守**：スタートアップ企業が厳格な規制遵守要件のある業界で事業を展開している場合、データの完全性を確保し、規制上の義務を果たすために、災害復旧計画が必要になることがあります。
- **クラウドサービスへの依存**：スタートアップ企業がクラウドサービスに大きく依存している場合、サービスの停止や中断が起こり得ることを認識してください。事業への潜在的な影響を評価し、これらのリスクを軽減するための災害復旧計画を検討します。

災害復旧の適切性を判断するためのパラメータには、以下のようなものがあります。

- **目標復旧時間（RTO）**：スタートアップが許容できるダウンタイムを定義します。迅速な復旧が重要な場合、確かな災害復旧ソリューションがより重要になります。
- **目標復旧時点（RPO）**：災害発生時の最大許容データ損失を決定します。このパラメータは、データバックアップの頻度とリカバリ処理の粒度に影響します。
- **費用対効果分析（Cost-Benefit Analysis）**：災害復旧計画への投資に対するダウンタイムの財務的影響を評価するために、費用対効果分析を実施します。潜在的な収益の損失とブランドの評判への影響を考慮してください。
- **リスクアセスメント**：サイバーセキュリティの脅威、自然災害、オペレーショナルリスクなど、潜在的なリスクを定期的に評価します。この情報をもとに、災害復旧戦略を見直し、更新してください。リスク管理の詳細については、第4章をご参照ください。

2.6.11 マルチゾーン、マルチリージョンの考慮

クラウドプラットフォームは、マルチゾーンやマルチリージョンアーキテクチャによる地理的な冗長性をスタートアップ企業に提供します。リージョン内の独立したデータセンターを活用したこれらの機能は、災害復旧戦略の堅牢性を高めます。

マルチゾーンアーキテクチャでは、各ゾーンが独立したデータセンターを表すため、同じ地理的なクラウドリージョン内で冗長性を確保することができます。このオプションは、クラウドリソースが同じリージョンにバインドされているため、通常は実装が簡単です。1つのゾーンに障害が発生した場合、ワークロードは自動的に同じリージョン内の別のゾーンにフェイルオーバーされるため、ダウンタイムを最小限に抑え、ビジネスの継続性を確保できます。

マルチリージョンアーキテクチャは、さらに複数のリージョンに冗長性を生み出します。このオプションはより複雑で、導入コストも高くなります。ですから、マルチゾーンであることは当初から考慮すべきことですが、マルチリージョンアーキテクチャに移行するには、さらに考慮すべきことがあります。

次のような場合のマルチリージョン戦略を考えます。

- **分散されたユーザーベース**：マルチリージョン戦略を採用することで、地理的に多様なユーザーベースにサービスを提供するスタートアップ企業の場合、異なるリージョン間でより低いレイテンシーとより優れたユーザーパフォーマンスが保証されます。
- **規制コンプライアンスとデータレジデンシー**：業種によっては、データ保存の要件が厳しい場合があります。特定のリージョン内でのデータ保存と処理を義務付ける規制（例えば、規制対象となる欧州連合（EU）の顧客にはEU地域からのみサービスを提供するなど）に準拠するため、マルチリージョン設定の採用を検討してください。
- **高可用性の要件**：高可用性と最小限のダウンタイムが要求されるクリティカルなアプリケーションには、SLAに応じてマルチゾーン構成が有効です。スタートアップ企業が成熟するにつれ、需要の高まりやコンプライアンスの必要性に基づいて、マルチリージョンアーキテクチャへの移行を検討することができます。
- **アーリーステージとコスト感度**：リソースと予算の制約が顕著なスタートアップ企業の初期においては、マルチリージョンのセットアップよりもマルチゾーンのセットアップの方が費用対効果が高い場合があります。スタートアップ企業の現在のニーズを評価し、ビジネスの成長に合わせてマルチリージョンアーキテクチャへの拡張を検討してください。
- **ゾーン/リージョンを超えたクラウドサービスレベル**：すべてのクラウドサービスがマルチリージョンデプロイメントを本質的にサポートしているわけではなく、特定のリージョン内でのみ高可用性を提供するものもあります。各サービスがサポートする可用性オプションを評価し、それらがお客様のレジリエンシー要件に合致していることを確認します。そのリージョン内でサービスが十分に利用可能であり、複数の地域にまたがる複雑な構成を必要としない場合、選択したリージョン内で堅牢なマルチゾーン設定に集中する方が、コスト効率が良く、運用効率も高い場合があります。

ほとんどのSaaSベースのスタートアップは、単一のリージョンでスタートしますが、冗長性のために複数のゾーンを使用します。ビジネス上の推奨事項は、主に個人情報保護法への配慮から、成熟期にはマルチリージョンデプロイメントを推進する可能性があります。フェーズ3では、リージョンやCSP（マルチクラウド）が追加されるかもしれません。

助言：成熟度段階への災害復旧の統合
スタートアップ企業は通常、最初のフェーズで1つのリージョンを展開し、DRの取り組みは特定の重要なデータの定期的なコールドバックアップから始めます。フェーズ2では、RTOを短縮するために、データタイプの追加と環境インフラストラクチャ（ネットワーク構成、ワークロード）のバックアップを行います。第 3 段階では、同じ CSP または別の CSP 上でアクティブ・アクティブ災害復旧を構築します。

2.7 データセキュリティ

クラウドプロバイダーは、複数の場所で複数の種類のストレージを使用しています。各ストレージタイプには、データ自体、場所、使用方法、アクセスのタイプ（読み取り、書き込み、更新、削除）といったいくつかの要因に基づく独自のセキュリティベストプラクティスがあります。ロケーションは、顧客ロケーション、サービスロケーション、使用タイプ、規制ニーズなどのビジネス要件に基づいて定義されます。

助言：前述したように、顧客の近くにデータを置くことはベストプラクティスですが、データには現地の法律や管轄区域が適用されることを忘れてはなりません。そのため、パラメータ（場所、法律、クライアント、アクセスの種類）を把握した上で、データ、アクセス、および場所を適切に計画します。これは、CDN、Obj、DBのどのタイプのストレージにも当てはまります。

2.7.1 ストレージの種類

2.7.1.1 ブロックストレージ

ブロックまたはボリュームストレージは、ブロックレベルのストレージを提供し、仮想環境において従来のハードドライブと同様に機能します。ストレージへの高速アクセス、オペレーティングシステムからのストレージの直接コントロール、ボリュームからのブート機能を必要とするアプリケーションには不可欠です。このため、データベースや複雑なトランザクションを使用するアプリケーションなど、低レイテンシーで高性能の読み取り/書き込み機能が必要な場合に最適です。

2.7.1.2 オブジェクトストレージ

オブジェクトストレージは、写真、ビデオ、文書などの膨大な量の非構造化データを扱うために設計されています。ファイル階層ではなく、フラットな名前空間内のオブジェクトとしてデータを保存するため、拡張性が高く、ウェブ上のどこからでもアクセスできます。このアプローチは、アーカイブ、データレイク、データバックアップ、ウェブコンテンツを直接ユーザーに提供する場合に最適で、耐久性、高可用性、ウェブアプリケーションとの容易な統合を実現します。オブジェクトストレージは、クラウド環境における重大なインシデントの原因となっており、コントロールの精査が求められています。

2.7.1.3 ネットワークファイルシステム

サーバーメッセージブロック（SMB）やネットワークファイルシステム（NFS）といった従来のネットワークファイルシステムのクラウド実装。主にレガシーアプリケーションやKubernetes実装の共有ドライブインフラストラクチャーに使用されます。ネットワークファイルシステムは、複数のクライアント

がネットワーク経由で同じシステムに同時にアクセスできるため、ファイル共有や同期アクセスが必要なシナリオに適しています。これらのシステムは、アクセス制御、クォータ、データ保護、コンプライアンススナップショットをサポートします。

27.1.4 コンテンツデリバリーネットワーク（CDN）

CDNは、様々な場所に戦略的に分散されたサーバーのネットワークで、地理的な位置に基づいてインターネットコンテンツをより効率的にユーザーに配信します。ウェブページ、動画、画像などのコンテンツをエンドユーザーに近いエッジサーバーにキャッシュすることで、CDNは遅延を減らし、ページのロード時間を短縮し、ユーザーエクスペリエンスを向上させます。CDNは、ウェブサイトアイテムへのアクセスやマルチクラウド、マルチリージョンのデプロイメントを管理する上で不可欠です。CDNはまた、DDoS保護、SSL/TLS暗号化、リアルタイム分析を提供し、配信パフォーマンスとセキュリティを確保します。

27.2 オブジェクトストレージの課題

オブジェクトストレージは広く利用されているクラウドサービスですが、特有なセキュリティ上の課題があります。本章では、これらの課題について詳しく説明します。

27.2.1 権限の不一致

- **定義**：オブジェクトストレージの認可はシンプルですが、難しいものです。それはインフラストラクチャ権限とアプリケーション認可の混合です。インフラストラクチャーレベルの権限で広範なアクセスが許可される一方で、アプリケーションレベルの認可で機密データへのアクセスが適切に制限されない場合、ミスマッチが発生する可能性があります。
- **データセキュリティの側面**：多くのセキュリティ事象は、オブジェクトストレージのパーミッションのガバナンスが不十分であることに起因しています。CSPのベストプラクティスを活用して、オブジェクトストレージセキュリティの正しい戦略を構築してください。

27.2.2 オブジェクト

- **定義**：クラウドコンピューティングにおける古くなったオブジェクトとは、クラウドに保存されているデータやオブジェクトのことです。
- **データセキュリティの側面**：古くなったオブジェクトは、セキュリティリスクを引き起こす可能性があります。最新のセキュリティ対策では保護されなくなった機密情報が含まれているかもしれません。不正アクセスやデータ侵害を防ぐために、これらのオブジェクトを特定し管理するには、定期的な監査とクリーンアッププロセスが不可欠です。

- **古いオブジェクトのアーカイブ/削除の自動化**：ストレージのバージョニングとオブジェクトのライフサイクルポリシーを実装して、古いオブジェクトの削除やアーカイブを自動化することで、このような問題を軽減し、露出の可能性を減らせます。

27.2.3 アーカイブ

- **定義**：アーカイブとは、アクティブに使用されなくなったデータを別のストレージスペースに移動し、長期保存することです。
- **データセキュリティの側面**：コンプライアンス上、アーカイブが必要になる場合があります。また、ランサムウェアや類似の脅威に対しても有効なコントロールです。アーカイブされたデータは、アクティブに使用されていないとはいえ、まだ機密である可能性があります。すべてのクラウドプロバイダーは、アーカイブされたデータを不正アクセスから保護し、データ保持に関する法律へのコンプライアンスを確保するためのポリシーを導入できるアーカイブサービスを提供しています。

27.3 データ分類

データの分類は、データセキュリティの主要な要素です。データの機密性に応じたセキュリティ対策を実施することが極めて重要です。暗号化、アクセス制御、モニタリングなど、必要なセキュリティコントロールを決定するために役立ちます。データは、その種類、機密性、組織にとっての価値に基づいて分類され、多くの場合、適切な取り扱いと保護を確実にします。

最初の段階から適切にデータを分類することで、SaaSベースのスタートアップは、データ漏洩防止計画などの成熟したデータ保護戦略の後の段階を構築することができます。

27.3.1 データ分類の方法

データ分類の方法は一般的に、データを特定し、その機密性と価値を評価した上で、事前に定義されたクラス（公開、内部、社外秘、機密など）に分類します。分類プロセスは、各分類の基準とそれに対応するセキュリティコントロールを定義したセキュリティポリシーによって導かれるべきです。これにより、機密データが露出するリスクを低減できます。

27.3.2 分類と感度

分類とは、データの種類、目的、組織にとっての重要性に基づいてデータを分類することです。機密性とは、データが許可なく開示、改ざん、破壊された場合に発生する可能性のある影響を指します。分類の幅は広がりますが、分類レベルの決定には感度が重要です。機密性の高いデータは、より厳格なセキ

ュリティコントロールが必要です。この違いを理解することで、潜在的な影響に基づく適切なセキュリティコントロールと保護要件を特定することができます。

27.4 暗号化と鍵の管理

27.4.1 転送中のデータは、常に業界で認められた強固な暗号化標準を使用して保護される必要があります。

システムとサービス間の通信は、適切な暗号化プロトコル（TLS 1.3など）を使用して機密性と完全性を確保する必要があります。クラウド環境へのアクセスは、トランスポートレイヤーセキュリティ（TLS）やインターネットプロトコルセキュリティ（IPSec）などのプロトコルを含む、セキュアなトランスポートメカニズムを活用する必要があります。ほとんどのクラウドプロバイダーは、TLS終端やVPNゲートウェイを含む組み込みの暗号化機能を提供し、認証局との統合による自動証明書管理機能を備えています。

27.4.2 保存中データの暗号化

すべてのクラウドプロバイダーは、保存中データの暗号化をサポートしています。保存中データの暗号化を正しく適用すれば、攻撃ベクトルとしてよく使われるバックアップやスナップショットを保護できます。スタートアップ企業が管理する一意の鍵（顧客管理鍵）で保存中データの暗号化をすることが重要です。ほとんどのクラウドプロバイダーは、共有暗号鍵サービス（AWSとGCPではKMS、AzureではKey Vault）を持っており、この配置はほとんどのデプロイメントで一般的です。

27.4.3 使用中データの暗号化

クラウドプロバイダーはコンフィデンシャルコンピューティングと呼ばれる技術を持っており、マシンのメモリ、データベース、コンテナを含む実行中のVMを暗号化する機能を提供しています。これにより、データやアプリケーションが特定の場所やハードウェアでしか処理できないようにすることが可能になります。コンフィデンシャルコンピューティングは、暗号通貨ウォレット、ブロックチェーン、軍事用実装のような機密性の高いワークロードで考慮されるべきです。

助言：ほとんどのスタートアップ企業は、運用コストが低く最小限のオーバーヘッドで運用が容易になるため、最初から移動中データと保存中データの暗号化を開始します。成熟するにつれて、スタートアップ企業は（顧客や環境を区別するために）さらに鍵を追加します。

27.5 SaaS利用者とBYOK（Bring-Your-Own-Key）について

SaaSプロバイダーとして、利用者はデータを暗号化するための暗号化鍵を最大限にコントロールできることを望んでいます。SaaSプロバイダーの中には、利用者がコントロールし、利用者のクラウドプロバイダーサービス（AWS KMS、Azure Keyvault、GCP KMS）にある鍵を使用して、利用者のデータを暗号化する機能を提供しているところもあります。これは良いセキュリティと保証プラクティスですが、利用者のデータが独自のVPC/バケット/データベースに分離されている特定のデプロイメントにのみ関連します。

助言：鍵管理のライフサイクルに関するCloud Security Allianceの調査は、その基礎を理解するために役立ちます。
Key Management Lifecycle Best Practices | CSA

2.8 アイデンティティとアクセス管理

今日のデジタル環境では、アイデンティティとアクセス管理（IAM）がサイバーセキュリティの要となっています。

IAMとは、人間も人間以外も、適切なタイミングで、適切な理由により、適切なリソースにアクセスできるようにする取り組みです。

デジタルアイデンティティを管理することで、IAMは、誰が自社のシステムにアクセスでき、そのシステム内で何ができるかをコントロールすることを可能にします。

本章では、クラウドのIaaS/PaaS環境におけるアイデンティティ管理に焦点を当てます。これは、クラウドインフラストラクチャー権限管理（CIEM）と呼ばれることもあります。

アイデンティティのアタックサーフェスは、SMB（スタートアップ企業を含む）であろうと大企業であろうと、すべてのセキュリティプログラムにリソースを割り当てる必要があるほど広範囲に及んでいます。

スタートアップ企業にとって、効果的なIAMは特に重要です。なぜならスタートアップ企業は機密データを扱ったり、クラウド環境に依存したり、サイバーセキュリティのリソースが限られている中で可用性の高いサービスを実行したりすることが多いからです。

2.8.1 IAMプラットフォームの進化

IAMの黎明期には、アクセス制御は単純で、基本的なユーザー名とパスワードの組み合わせで十分なオ

ンプレミスのシステムに限定されることがよくありました。企業ネットワークの増加に伴い、企業は一元化されたIAMシステムの必要性を認識し始めました。この時期に、役割ベースのアクセス制御（RBAC）が誕生しました。これは、ユーザーの役割に基づいて権限をグループ化し、アクセスの割り当てと監視を容易にするものです。RBACは瞬く間に企業環境の標準となり、構造的でありながら柔軟なアクセス制御を実現しました。

クラウドコンピューティングへの移行はIAMに変革をもたらし、リモートアクセス管理、サードパーティの統合処理、分散環境にわたる膨大なデータの保護といった複雑な課題をもたらしました。このシフトは、効果的なIAMの基本原則としてのIAAA（Identification、Authentication、Authorization、Accountability）の強化を企業に促しました。市場の製品とソリューションは適応し、オンプレミスのハードウェア中心のシステムから、よりダイナミックなソフトウェアベースのクラウドIAMソリューションへと進化しました。属性ベースまたはポリシーベースのアクセス制御（ABAC/PBAC）のようなアクセスモデルが登場し始め、ユーザーの場所、デバイス、時間などのコンテキストに基づいて、より細かいアクセス制御が可能になりました。

IAMは進化を続けており、ゼロトラストやアダプティブ認証などのイノベーションが注目を集めています。

IAMの進化に伴い、アタックサーフェスは拡大しています。当初、アイデンティティ攻撃は、ハッカーが脆弱なパスワードを推測することや、フィッシング詐欺を使ってユーザーを騙してクレデンシャルを漏洩させるという単純な手法から始まりました。

デジタル環境が高度化し、IAMセキュリティがそれに伴って進歩するにつれて、攻撃者はブルートフォース攻撃、クレデンシャルスタッフィング、ソーシャルエンジニアリングといった、より洗練されたテクニックに変わっていきました。これらの手法により、攻撃者は従来の防御を迂回し、企業がユーザーアカウントやアクセスポイントを保護する方法のギャップをエクスプロイトすることができました。

今日、脅威にさらされているのは人間のアイデンティティだけではありません。サービスアカウント、AIエージェント、ボット、IoTデバイスなど、人間以外のアイデンティティが悪意のあるアクターに狙われるケースが増えています。これらのアイデンティティは、多くの場合、広範なアクセス権を持っていますが、常に同じレベルのセキュリティ監視を受けるわけではないため、標的になりやすいです。攻撃者は、これらのアカウントの脆弱な設定、見落とされたアクセス許可、制限されたモニタリングをエクスプロイトして、不正アクセスを実行し、ネットワーク内を移動します。その結果、人間と人間以外の両方のアイデンティティを保護することが重要になっており、それぞれに固有の課題とリスクがあります。スタートアップ企業は、IAM技術が進化するにつれて、アイデンティティベースの攻撃の手口や標的も進化することを理解し、警戒を怠らない必要があります。

28.2 クラウドアイデンティティの理解

スタートアップは、人間や人間以外の複数のアイデンティティへのアクセスを決定します。人的アイデンティティとは、クラウドアプリケーション、データ、インフラストラクチャへのアクセスを必要とする従業員、請負業者、または管理者を指します。最も高いアクセスレベルを持つルートアカウントは、主に複数の人間に提供されるため、もう1つの重要な考慮事項です。
人間以外のアイデンティティには、クラウド環境とやり取りするアプリケーション、VM、マイクロサービスを表すサービスアカウントとマシンアイデンティティが含まれます。これらのアイデンティティは、自動化されたタスクを実行することが多く、過度に広範な権限が付与されることが多いため、適切に管理されていない場合は魅力的な標的となります。

クラウドには、人間か人間以外かを問わず、多くのアイデンティティが散在しているため、スタートアップは初日から最小特権と職務分掌のセキュリティ原則を採用する必要があります。最小特権の原則（POLP）は、従業員が業務を完了するために必要なアカウント権限を提供し、それ以上の権限は提供しません。職務の分離には、責任、アクセス、権限の分割が必要です。

助言：IaaS/PaaSプラットフォームは階層構造で管理されます。しかし、最上位レイヤーには、高い権限を持つアカウント（Azureグローバル管理者とAWSルートアカウント）が存在します。これらのアカウントは、ベストプラクティスに従って慎重に管理されるべきです。

AWS root user best practices

Azure secure privileged access

GCP privilege access

28.3 IdPの役割

IaaS/PaaSのCSPは、組織のユーザーディレクトリとして機能するようには設計されていませんし、そうあるべきでもありません（AzureのEntra IDは例外です）。組織内のユーザーディレクトリは、ユーザーの識別情報を管理・保存し、認証サービスを提供する専用システムまたはサービス上に存在すべきです。これがアイデンティティプロバイダー（IdP）となります。その主な機能は、個人のアイデンティティを確認し、その個人に関する情報を他のサービス、アプリケーション、またはシステム（クラウドプラットフォームや基盤となるアプリケーションを含む）に提供することです。

一元化された IdP は、すべてのアイデンティティの一元的な表示、ポリシーの実施、オンボーディングおよびオフボーディングプロセスの自動化、アイデンティティ監査アクションのための 1 つの場所など、多くのセキュリティおよび運用上の利点を提供します。IdPの適切な使用は、多くのセキュリティ上の課題や顧客の疑問をカバーします。

すでに導入されているIdPを使用するか、一元化されたIdPを導入することで、組織全体でアイデンティティを過剰に管理する必要性を回避し、複数のアプリケーションやプラットフォーム（ユーザーアカウント）のアイデンティティを単一のエンティティ（個人）として統合できます。

人気のあるアイデンティティプロバイダーには、Okta、Microsoft Entra ID、Google Workspace、OneLogin、Ping Identity、Cyberarkなどがあります。

一般に、IdP は、全社的な権威あるデータソース（個人に関する属性を含み、この情報の主要なまたは最も信頼できるソースとみなされるリポジトリまたはシステム）と同期されるべきです。通常、これは組織のヒューマンキャピタル管理（HR）システムで、HiBobやWorkDayなどが含まれます。

助言：SaaS利用者は、SAMLのようなアイデンティティフェデレーションサポートを要求することがよくあります。そのため、SaaSベースのスタートアップアプリケーションは、最初の段階から一般的なIDPを使用したSSOをサポートする必要があります。

助言：スタートアップ企業は、IDPの属性（Active Directoryのグループなど）をCSPのロールにマッピングすることで、オンボーディングとオフボーディングの認可決定を自動化できます。例えば、Tutorial： Configure AWS IAM Identity Center for automatic user provisioning

28.4 認証と条件付きアクセスポリシー

基本的な認証タイプは、通常、ユーザー/パスワードのような「あなたが知っているもの」です。
現在、ほとんどの規制やベストプラクティスは、パスワード認証のセキュリティは十分でないとし、第二の要素、通常は「あなたが持っているもの」を推奨しています。最も一般的な要素は、ハードウェアトークン（Yubikey、Duoなど）のような物理的なデバイス、またはインストールされた認証アプリ（Duo、Authenticatorなど）を通じてワンタイムパスワードを受け取ることができるスマートフォンです。ほとんどのクラウドプロバイダーは最近、FIDO/パスキーのような最新のプロトコルを実装しています。また、クラウドのログインプロセスにバイオメトリクス認証を統合することもできます（"あなた自身を示すもの"）。

ほとんどの場合、スタートアップ企業はパスワードとスマートフォンアプリに基づく二要素認証（2FA）を全ユーザーに提供することから始めます。簡単で追加費用もかかりません。スタートアップ企業が成長するにつれ、特権アカウント（root、グローバル管理者など）が増えるため、ハードウェアベースの多要素認証（MFA）を実装する必要があります。

今日、ほとんどのIdPは、認証プロセスで追加の要素を使用して、追加のアクセスの決定を行うことを許可しています。これは条件付きアクセスまたは属性ベースのアクセス制御（ABAC）と呼ばれます。ABACでは、スタートアップはエンリッチポリシーを定義して、認証方法の複雑さを強制したり（つまり、別の認証要素を要求したり）、多数のセッション属性に基づいて認可を制限したりします。
いくつか例を挙げます。

- いつ（例：ユーザーが勤務時間外にログインしたなど）

- 送信元IP（例：地域外からログインしたユーザー）
- ターゲットIP（例：初めてターゲットにアクセスしようとするユーザーなど）
- 送信元デバイス（例：ユーザーが使用したことのないデバイスからアクセスしている、またはユーザーが会社から支給されていないデバイスからアクセスしているなど）

助言：テキストメッセージ（SMS）に基づくMFAは、SIMスワップなどの様々な攻撃のために安全でないと考えられています。したがって、私たちは他の認証方法を好みます。
NIST Denounces SMS 2FA - What are the Alternatives? - SecurityWeek

28.5 認可

認可は、役割、グループ、または属性など、ユーザーに割り当てられた特定の割り当てに基づいて、システム内のアイデンティティアクセスを決定します。

クラウド環境では、リソースのセキュリティ、コンプライアンス、適切な機能を確保するために、認可を効果的に管理することが極めて重要です。

すべてのIaaS/PaaSプロバイダーは、人間と人間以外に適切な権限を与えるために、さまざまな組み込みおよびカスタムのロール、グループ、ポリシー、スキームをサポートしています。認可を管理するプログラムと手段は、スタートアップが成長し、ユーザーやサービスアカウントなどのアイデンティティが増えるにつれて変化します。

アイデンティティが外部ディレクトリで管理されている場合、外部属性とクラウドの許可／ロールとのマッピングが必要であり、通常はIdPが行います。これは通常、クラウドプロバイダーの役割を特定のIdPグループにマッピングすることで実現されます。

28.6 IAMの監査

アイデンティティとその活動の監査は、コンプライアンスを確保し、異常を検出するために、アプリケーションまたはシステム内の人間および人間以外の行動を追跡し、レビューすることを含みます。これは主に、手動監査、監査ログの収集、または専用のツール/プラットフォームを使用して行われます。

手作業による監査では、多数の機密プラットフォームにわたるアイデンティティ、アクセス、アクションをレビューし、権限が要件およびアクションと一致していることを確認します。
アクティビティログを収集することで、アイデンティティのアタックサーフェスとさまざまな脅威シナリオに対する検出および対応能力を確立するための基盤が構築されます。

できれば毎月、不可能であれば少なくとも四半期に一度、アクセス権を見直し、更新し、過剰なアクセ

ス権を削除するアクセスレビューのスケジュールを確立することから始めましょう。

アクティビティのロギングと収集については、クラウド、アイデンティティ、サードパーティの各プラットフォームでロギング機能を有効にして、ログイン、アクセス試行失敗、重要なリソースで実行されたアクションに関するデータを収集することから始めます。これらのログをセキュアで一元化された場所に保存します。これは、最初はオブジェクトストレージで、後に分析ツールのデータベースになります。

また、連続したログインの失敗、危険なログイン場所や時間帯、その他の関連指標など、通常とは異なるアイデンティティのアクティビティに対するアラートを早期に設定することで、チームは疑わしい行動を早期に検出できます。

28.7 IAM導入のフェーズ

IAMサービスの成熟は、多くの場合、次のようなものです。

- **フェーズ 1:** 従業員の数は非常に少なく、その結果、アイデンティティや役割も少ない。このフェーズでは、成熟したオペレーション部門（DevOps）は通常存在せず、開発・テスト環境と本番環境では主に役割が分かれています。役割は必要不可欠であり、手動で割り当てられます。アクセス制御は多くの場合、フラットで集中管理され、監視は最低限しか行われず、セキュリティ対策は基本的には手作業によるレビューに依存しています。ユーザーのオンボーディングとオフボーディングは通常手動で行われます。認証は最初からMFAにすべきです。
- **フェーズ 2:** より多くのユーザー、サービス、環境が追加され、より多くのロールが追加されます。開発、テスト、本番の分離は成熟しているはずです。オンボーディングとオフボーディングは部分的に自動化され、通常は集中型IdPを使用します。本番環境での役割は、製品コンポーネントごとに分離され、必要なときにのみ使用され、慎重に管理されるべきです。すべてのリソースには、アクセスの判断に役立つようにタグを付ける必要があります。RBACはよりきめ細かくなり、サービスレベルのパーミッションは環境間でより厳しく実施されます。
- **フェーズ 3:** IAMはもう成熟しているはずです。成長には自動化とガバナンスの強化がつきものです。ロールのプロビジョニングを含む、オンボーディングとオフボーディングのプロセスは自動化されています。特権ユーザーはすべて厳重にモニタリングされ、強制されます。ロールは最小特権に調整され、定期的なアクセスレビューが行われます。この時点で、スタートアップ企業はPIMソリューションやIdentity Governance and Administration（IGA）ツールを導入して、クラウドアプリケーションやプラットフォームに必要な全体的なアイデンティティとアクセスの管理を容易にします。定期的なアクセスレビューとコンプライアンスチェックの設定は必須です。

助言：すべてのクラウドプロバイダーは、特権ユーザーのリスクを軽減するための手続きを持っています。これには管理が必要です。ユーザー認証、認可、およびアクセス手順は以下のようです。
AWS Assume role, Azure privileged access, or GCP just-in-time

2.8.8 サービスアカウントとシークレット管理

サービスアカウントは、アプリケーションやワークロードがクラウドのリソースやアクション（APIコール、アプリケーションの実行、バッチ、スクリプトの実行）を使用またはアクセスするためのアイデンティティです。サービスアカウントには、その機能をコントロールする固有のユーザー名、ロール、権限があり、クラウドサービスは多くのサービスアカウントを使用します。サービスアカウントは、最小特権や監視されたアクセスなど、IAMと同じ原則に従わなければなりません。最も大きな違いは認証プロセスで、人間が関与しないため、MFAや同様のソリューションを利用することはできません。サービスアカウントが認証する方法は、しばしばアプリケーションシークレットと呼ばれます。

シークレットは、ホストされたデータやアプリケーションの機密性、完全性、可用性を確保する上で重要な役割を担っており、非常に一般的な攻撃ベクトルと考えられています。

シークレットには、アクセス鍵（認証クレデンシャル）、暗号鍵（データの暗号化と復号化に使用）、機密データなどがあります。非常にありがちな間違いは、設定ファイルにコードと一緒にシークレットを保存することであり、これは鍵の露出につながります。

2.8.8.1 シークレット管理シナリオの例

アプリケーションのシークレットをセキュアに保管するための推奨事項は、以下のようにシナリオによって変わります。

- クラウド環境**内から**クラウドリソースへのアクセス：
  - このシナリオでは、静的なアクセス鍵の使用は、インスタンスのロールを仮定するような、よりセキュアなソリューションに置き換えることができます（AWSインスタンスロールまたはGCPとAzureのAzureワークロードアイデンティティフェデレーション）。
- クラウド環境**内から**外部サービスへのアクセス：
  - このシナリオでは、シークレット管理のための指定ソリューションで鍵を保護します。お使いのクラウドプラットフォームツール（Azure key vault、AWS/GCP Secrets Manager）を使用するか、HashiCorp Vault、CyberArk Conjur、Akeyless secret manageなどのおなじみのサードパーティツールを使用することができます。
- クラウド環境の**外部**（利用者ネットワークやオンプレミスなど）**から**内部クラウドリソースへのアクセス
  - このシナリオでは、シークレットのセキュアな保存は、外部で利用可能なツールに依存

します。シークレット管理ソリューションがあれば、それを使うべきです。ただし、長期的な静的な鍵を使用する場合は、長期的な補完的コントロールを行う必要があります。

- このシナリオでは、IdPを使用した短期間の短期トークンが活用されるのが理想的です。クラウドプロバイダーは、Short Term Tokens (STS)やAzure Shared Access Signature (SAS)のような複数のテクニックを使用しています。

助言：AWSはIAMに対してきわめて細かい粒度のアプローチを提供しています。リソースへのアクセスはデフォルトで禁止されており、複数のポリシーとロールを設定することで、リソースへのアクセスをきめ細かく制御し、サードパーティのIdPと上手く統合することができます。しかし、スタートアップ企業は、それらのロールとポリシーをすべて設定、管理、開発しなければなりません。AzureとGCPは、デフォルトのアクセスレベルを持つ事前定義の組み込みロールを備えた、より一般的なアプローチを採用しています。AzureとGCPは、独自のIdPの特性にも大きく依存しています。

2.9 クラウドワークロードのセキュア化

Cloud Security Allianceは、ワークロードを「仮想マシン、コンテナ、その他の抽象化されたものにおける処理の単位」と定義しています(出典：Security Guidance for Critical Areas of Focus in Cloud Computing)。クラウドベース環境への移行は、ワークロードの種類（コンテナ、サーバーレスエマージ）を変化させ、これらのワークロードのデプロイ、スケーリング、保守の方法に革命をもたらしました。
ワークロードの管理は、あらゆる規模の企業にとって業務の成功に不可欠です。クラウドコンピューティングへの移行は、リソース利用の最適化、セキュリティとコンプライアンスの確保、高可用性とパフォーマンスの維持など、ワークロード管理における新たな課題ももたらします。

以下では、ワークロードをセキュアにするために必要な手順を示します。

助言：SaaSベースのスタートアップ企業にとって、エンドポイントプロテクションソフトウェア、またはSOARとアンチウイルスの組み合わせをインストールすることは、公開されていない、または外部ファイルを処理しないアプリインスタンスであっても、一般的なプラクティスです。このようなケースでマルウェア対策が有効であるかどうかは議論の余地がありますが、SaaSベースのスタートアップ企業は数多くの監査に直面しており、監査人にマルウェア対策が不要である理由を説明するよりも、ソフトウェアをインストールする方が簡単であることがよくあります。

2.9.1 ハードニングされたイメージの使用

ほとんどすべてのワークロードは、デプロイするイメージから始まります。VMであれコンテナ化されたアプリケーションであれ、クラウドベースのソリューションを展開する場合、ワークロードのセキュリティを確保する責任はクラウド利用者にあります。これには、ソフトウェアやサードパーティパッケージの安定した最新バージョンをイメージに適用し、脆弱性を徹底的に排除し、定期的なセキュリティスキャンを実施することが含まれます。クラウドサービスは動的な性質があるため、これらの機能を自動化することをお勧めします。

スタートアップ企業には、最初から基本的なハードニングしたゴールデンイメージを作成することをお勧めします。次のフェーズに成熟すると、スタートアップ企業はイメージを追加し（テスト/開発/本番やアプリケーションコンポーネント用の異なるイメージなど）、しばしばCI/CDパイプラインの一部と

してイメージの作成とハードニングの自動化を進めます。

助言：Center for Internet Security (CIS) は、すべての主要なCSP上で事前に設定されたハードニングされたイメージを提供しています。これらのイメージはCIS標準に準拠しており、アシュアランス要件（テスト環境と本番環境など）に基づく2つのハードニングレベルを提示しています。

イメージはベースラインとして使用することができ、作業負荷の要件に応じて変更する必要があります。追加のイメージは通常、CSPマーケットプレイスで入手できます。

29.2 脆弱性とパッチ

インスタンスの脆弱性をスキャンすることで、ハードニングやパッチ管理プログラムをサポートすることができ、世界中の標準や規制で義務付けられています。脆弱性管理サービスは、セキュリティ評価を自動化し、潜在的な脆弱性を特定し、クラウドインフラストラクチャーのセキュリティポスチャを強化するための実用的な推奨事項を提供します。クラウドのワークロードは、新しいタイプのワークロード（コンテナ、Function-as-a-Service、サーバーレス）を利用するため異なっており、脆弱性管理ツールはこれらのタイプのワークロードもカバーする必要があります。この種のツールは、CloudWorkload Protection Platforms（CWPP）と呼ばれています。

脆弱性を検出した後は、パッチや修正プログラムをインストールする必要があります。パッチ管理ツールは、CWPPツールに統合することも、個別に管理することもできます。SaaSベースのスタートアップ企業は、脆弱性のリスクに基づき、脆弱性の検出とパッチ適用にかかる平均時間をできる限り短縮するよう努力すべきです。パッチ管理の手順は、ダウンタイム、コントロールされた展開、インストール後の正常性テストとセキュリティテストを考慮する必要があります。

助言：すべてのCSPは、AWS Inspector、Azure Defender for Cloud、GCP Security Command CenterなどのCWPP用のネイティブツールを備えています。

すべてのCSPは、ネイティブのパッチ管理ツールを備えています：AWS System Manager、Azure Update Manager、またはGCP VM Manager。

29.3 Kubernetesのセキュリティ

Kubernetes（k8s）の使用は、コスト削減とリソースの最適化により、SaaSベースのスタートアップ企業で非常に人気があります。さらにK8sは、アプリケーションの迅速なデプロイメントとスケーリングを可能にすることで、俊敏性と開発スピードを向上させ、企業が市場の需要に応えて新機能や新サービスをより迅速に提供できるよう支援します。

K8sはスタンドアロン/非マネージドとして実装できます。それでも、すべてのクラウドプロバイダーはマネージドKubernetesサービスを提供しており、Kubernetesクラスタの管理を簡素化し、自動アップデート、セキュリティパッチ、他のクラウドサービスとの統合などのメリットを提供しています。

29.3.1 K8sのランタイムセキュリティ

コンテナの特性と成熟度により、アクティブコンテナ用のランタイムセキュリティソリューションを追加することが推奨されます。その目的は、コンテナ環境特有の悪意のある活動を検出し、防止することです。コンテナセキュリティランタイムは通常、CWPPツールの一部です。

ランタイムセキュリティの予防コントロール

- SeccompはLinuxカーネルの強制ツールで、コンテナからホストへのシステムコールを制限することができます。例えば、SYS_TIMEシステムコールはホストから現在の時刻を返します。このシステムが他のシステムを呼び出し、ブロックすることを許可するポリシーを使用することができます。Seccompの詳細については、Kubernetes best practices for securityを参照してください。
- SELinux/AppArmorは、コンテナを制限できるLinuxカーネルセキュリティモジュールです。このソリューションでは、コンテナをそのファイルだけに制限し、他のプロセスからのアクセスを防ぐことができます。コンテナが侵害されれば、アタックサーフェスが限定されます。これは、ファイルやプロセスにコンテキストを設定し、プロセスが何を見たり変更したりできるかを強制するポリシーを定義することで行います。
- コンテナにSELinuxラベルを割り当てるには - Configure a Security Context for a Pod or Containerを参照。

ランタイムセキュリティの検出コントロール

- Falcoはオープンソースのランタイムセキュリティスキャナーで、特定のシステムコールの動作に警告を発するために使用することができます。例えば、コンテナがホスト上に新しいディレクトリを作成するために mkdir システムコールを実行しようとするたびに、アラートをトリガーします。
- クラウドプロバイダーは、ネイティブのランタイム検出サービスを提供しています。これらのサービスは、既存のクラウドインフラストラクチャーとシームレスに統合できるように設計されており、リアルタイムのセキュリティモニタリングと脅威検出機能を提供します。このようなサービスの例としては、Amazon GuardDutyやMicrosoft Defender for Cloudなどがあります。

29.3.2 クラウドプロバイダーのネイティブKubernetesセキュリティサービス

前述のように、スタートアップの間で最も人気のあるオプションは、クラウドプロバイダーのネイティ

ブKubernetesセキュリティサービスを利用することです。AWSはこれらのサービスをAmazon Elastic Kubernetes Service (EKS)を通じて提供し、脅威検出のためのAWS GuardDuty、セキュリティ標準準拠のためのAWS Security Hub、自動セキュリティ評価のためのAmazon Inspectorなどのツールで補完しています。Microsoft AzureのKubernetesセキュリティは、Azure Kubernetes Service（AKS）を中心に、高度な脅威防御と継続的な健全性監視を提供するMicrosoft Defender for the cloudによって強化されています。また、コンプライアンスを実施するためにAzure Policyを利用し、包括的なロギングとパフォーマンスメトリクスのためにAzure Monitorを利用します。Google Kubernetes Engine（GKE）向けのGCPのセキュリティフレームワークには、統合セキュリティ管理、リスク評価のためのSecurity Command Center、コンテナデプロイメントにおけるリアルタイムの脅威検出のためのContainer Threat Detectionが含まれます。さらに、GCPはGoogle Cloud Operations Suiteを提供し、Kubernetesワークロードの可視性とコントロールを強化します。AWS、Azure、GCPによるこれらのネイティブサービスは、Kubernetesに特化したセキュリティレイヤーを提供し、クラウドセキュリティとコンプライアンスのベストプラクティスを遵守しながら、コンテナ化されたアプリケーションをさまざまな脅威から確実に保護します。

助言：

- EKS上のマルチテナントアプリケーションのためのAWSガイドライン
- k8sサービスのコンフィギュレーションは、業界標準に基づいてハードニングされるべきです。CISには、非管理下および管理下のデプロイメントでk8sをハードニングするためのガイドがあります。
- Kube-benchは、KubernetesのCISベンチマークチェックを自動化するためのオープンソースツールです。

29.4 サーバーレスとFaaS

サーバーレスまたはFaaS（Function as a Service）のバリュープロポジションには、俊敏性、革新性、サーバー管理タスクの排除が含まれます。企業はサーバーレスソリューションを利用することで、コンピュートノードの管理オーバーヘッドを削減し、ビジネス価値に集中することができます。サーバーレスセキュリティの利点は以下の通りです：

- **運用負荷の軽減**：サーバーレスプラットフォームは、セキュリティパッチやアップデートを含め、基盤となるインフラストラクチャを自動的に管理します。これにより、サーバーレスアプリケーションは、手動による介入なしに、セキュアで最新の環境で実行されます。
- **アタックサーフェスの削減**：サーバーレスアーキテクチャは、基盤となるインフラストラクチャを抽象化し、潜在的な攻撃者のアタックサーフェスを削減します。例えば、FaaS（Function as a Service）では、アプリケーションコードのセキュリティ確保と必要な権限の設定だけに集中すればよく、プロビジョニング、スケーリング、ハードニングなどのインフラストラクチャーセキュリティと運用のタスクはクラウドプロバイダーの責任とできます。

- **組み込みの認証と認可**：クラウドプロバイダーのアイデンティティとアクセス管理（IAM）により、サーバーレス機能へのアクセスをコントロールできます。特定のサービスやリソースへのアクセスを制限する、きめ細かいパーミッションを定義できます。
- **拡張性**：サーバーレスプラットフォームは、需要に応じてリソースを自動的にスケールします。この弾力性により、アプリケーションはさまざまなワークロードを効率的に処理できます。

助言：Cloud Security Allianceは、サーバーレスアプリケーションに対する脅威のトップランキングを発表しました：The 12 Most Critical Risks for Serverless Applications | CSA

29.5 CI/CDパイプラインのセキュリティ

多くのSaaSベースのスタートアップは、さまざまな自動化とセキュリティテストのレベルでCI/CDパイプラインを実装しています。この章では、CI/CDパイプラインのセキュリティについて詳しく述べ、アプリケーションセキュリティの章では、パイプライン内部のセキュリティゲートとテストについて詳しく述べます。

CI/CDパイプラインが直面する潜在的な脅威を理解することは、スタートアップにとって非常に重要です。パイプラインコンポーネントは、多くの機微なサービス（コードリポジトリや本番環境など）と相互作用があります。脅威には、未認可なコード変更、セキュアでない依存関係、危険なビルド環境などがあります。さらに、不十分なアクセス制御、暗号化されていない通信、脆弱な認証メカニズムも重大なリスクとなります。クラウドベースのスタートアップは、柔軟性のあるセキュリティ戦略を策定するために、これらの脅威を評価し、優先順位を付ける必要があります。

クラウドワークロードにおけるCI/CDパイプラインの主なセキュリティコントロールには、以下が含まれます。

- 制限されたアクセス制御：CI/CDパイプラインインフラストラクチャーへのアクセスを許可された担当者のみに制限します。強力な認証メカニズムと役割ベースのアクセス制御(RBAC)を導入し、正当な必要性のある人だけがパイプラインやその設定を変更できるようにします。
- 監査証跡とモニタリング：すべてのCI/CDパイプライン活動の包括的なログを維持します。リアルタイムのモニタリングソリューションを導入し、異常なアクティビティや未認可な変更を検出して警告します。
- イミュータブルな監査ログ：監査ログが変更不可能であり、変更できないことを確実にします。これにより、調査およびコンプライアンス目的のための信頼できる活動記録が提供されます。
- パイプラインの構成管理：パイプライン設定をコードとして扱い、バージョンコントロールで管理します。これには、パイプラインのコンフィギュレーションを変更する際の厳格なレビュープロセスも含まれます。
- パイプラインインフラストラクチャーの定期的なセキュリティスキャン：CI/CDパイプラインイ

ンフラストラクチャーの脆弱性を定期的にスキャンします。これには、パイプラインプロセスで使用されるサーバー、コンテナ、その他のコンポーネントが含まれます。

- 機密データの暗号化：暗号化により、クレデンシャルや設定ファイルなど、CI/CDプロセス内の機密データを、転送中と保存中の両方で保護します。
- セグメンテーションとアイソレーション：CI/CDパイプラインインフラストラクチャーを他のネットワークやシステムから分離します。ネットワークセグメンテーションとファイアウォールルールを使用してトラフィックをコントロールし、潜在的な攻撃ベクトルを制限します。
- 機能（生産や開発など）に応じてパイプラインを分離し、攻撃の影響範囲を限定します。
- バージョン管理とロールバック機能：パイプライン構成のバージョン管理を行い、セキュアでない構成や欠陥のある構成が導入された場合のロールバック機能をサポートします。これにより、セキュリティの設定ミスが発生した場合でも、迅速なリカバリが可能になります。
- 災害復旧とバックアップ計画：CI/CDパイプラインは、堅牢なバックアップと災害復旧手順を備えている必要があります。これらの手順により、セキュリティ侵害やその他の障害が発生した場合の事業継続性と迅速なリカバリを確実にします。
- インシデントレスポンス計画：CI/CDパイプラインのインシデントレスポンス計画を策定し、定期的に更新します。チームがセキュリティインシデントに効果的に対処できるよう訓練されていることを確認します。
- 継続的なセキュリティトレーニングと意識向上：最新のセキュリティ脅威とベストプラクティスに関する最新情報をチームに提供します。定期的なトレーニングにより、パイプラインのセキュリティを維持する上での自分の役割を全員が認識するようにし ます。

助言：OWASP Top 10 CI/CD Security Risksは、一般的なCI/CDプラクティスに関する有益な情報を提供します。

2.10 モニタリング、監査、フォレンジック

2.10.1 クラウドモニタリングの種類

スタートアップのクラウド環境を継続的にモニタリングすることは、SLAを維持し、サービスの途絶を回避し、さまざまなセキュリティ基準や規制を遵守するために極めて重要です。クラウドモニタリングオプションには以下のものがあります：

- **健全性とパフォーマンスのモニタリング**：運用上の理由によるもの（セキュリティモニタリングとは対照的）。フェーズ1では、スタートアップは通常、基本的な障害を検出するために、組み込みのクラウドプロバイダーのサービスを利用します。成熟するにつれて、多くの場合オープンソースのツール（Prometheusなど）を使用して、追加のメトリクスとログが収集され、分析されます。フェーズ3で、デプロイメントやクラウドプラットフォームの数が増えてくる場合は、一部のスタートアップ企業はおそらく商用モニタリングソリューション（Datadog、Zabbix、Logz.ioなど）を導入するでしょう。このモニタリングについては、この文書では詳しく説明しま

せん。

- **セキュリティポスチャのモニタリング**：ポスチャ管理とは、組織のクラウドコンピューティング環境の全体的なセキュリティ状態やスタンスを指します。環境の設定は定期的にチェックされ、設定ミスやコンプライアンス上の課題がないか分析されます。詳しくは以下のパラグラフをご覧ください。
- **セキュリティログの収集と分析**：セキュリティログの収集は、情報セキュリティの基本的な概念であり、検知、緩和、フォレンジックに必要です。ほとんどの規制やベストプラクティスは、これを主要な要件として挙げています。詳細は次の段落で述べられています。

助言：モニタリングに関してスタートアップ企業が直面する最大の課題は、24時間365日の継続的な監視体制と、モニタリングや分析を行う専門スタッフの不足です。フェーズ1では、スタートアップ企業は通常24時間365日のサービスを提供していませんが、成熟するにつれて、通常は外部のマネージドサービスプロバイダー（MSSP）を利用して24時間365日のサービスを提供するようになります。

2.10.1.1 セキュリティポスチャ管理について

ポスチャ管理機能は、スタートアップ企業がクラウド環境におけるセキュリティ脅威を検出、分析、対応するための主要な要素です。また、顧客のレビューや質問、監査に対応する上でも重要です。適切なポスチャ管理の展開により、スタートアップ企業は以下を実行できます。

- **設定ミスを検出**：これらは、セキュリティの脆弱性、機密データの漏洩、不正アクセスにつながる可能性があります。
- **イベントへの対応**：アラート、自動修復、またはワークフローの開始
- **コンプライアンス保証**：クラウド構成を業界の規制や標準に合わせ、コンプライアンスに反する構成項目に対して警告を発します。

スタートアップ企業は次のような場面でポスチャ管理を活用します。

- **継続的なサービス**：スタートアップ環境における設定ミスやリスクを継続的に検知し、社内導入またはフォースパーティのサービスとして利用
- **1回限りの監査**：環境の現状を評価するためのアドホックなスキャン。これは通常、顧客の保証要求や規制要件に対応するために行われます。

注：CSPMツールによって収集される情報は、データ収集の直近24時間のものである可能性があり、必ずしもリアルタイムのデータとは限りません。

2.10.2 Cloud Native Application Protection Platform (CNAPP)

Cloud Native Application Protection Platform（CNAPP）は、IaaS/PaaS環境およびクラウドネイティブ

アプリケーションを展開する顧客のために設計されたツール群です。CNAPPツールは、組織のポスチャを見直し、洞察を提供することに重点を置いています。CNAPPは、スタートアップ企業が標準や規制を遵守し、セキュリティの設定ミスを検出し、クラウド環境を管理できるよう支援します。CNAPPの主な構成要素は以下の通りです。

- Cloud Security Posture Management（CSPM）：IaaS/PaaSクラウド環境のポスチャを検出します。CSPMはCNAPPポートフォリオの主要ツールであり、ポスチャーモニタリングの旅を始める場所です。
- Data Security Posture Management（DSPM）：組織のデータサイロの発見、分類、保護、モニタリング
- Cloud Infrastructure Entitlement Management （CIEM）：クラウドIaaS/PaaS環境内のアクセス権と権限を管理および監視します。
- Application Development Security Posture（ASPM）：スタートアップ企業は、クラウドを利用して独自のソフトウェアを開発・展開しています。ASPMソリューションは、セキュアなアプリケーション開発と展開に関連するセキュリティゲートとプロセスを編成します。

スタートアップ企業は、クラウドプロバイダーにビルトインされたCSPMツール（AWS security hub、GCP Command Center（実際の利用にはプレミアムライセンスが必要）、 Azure security center、MS Defender for Cloudを使って第1フェーズを開始し、基本的なルールを有効化し有能な従業員にアラートを割り当てます。フェーズ2の成熟に伴い、スタートアップ企業はより多くのチェックとルールを導入し、適切なセキュリティと開発スキルを持つ関連担当者にモニタリングを割り当てます。第3フェーズでは、スタートアップは24時間365日の外部モニタリングサービスに移行することがよくあります。マルチクラウドの採用アプローチにより、スタートアップ企業は通常、Palo Alto Prisma、Check Point Cloud Guard、Wiz、Orcaなどのサードパーティ製ツールに切り替えています。

210.3 IaaS/PaaSログ管理

ログの収集と分析は、セキュリティ標準とベストプラクティスの要です。適切なログ管理の実施には、変更の追跡、セキュリティイベントの検出、規制への準拠などが含まれます。IaaS/PaaSプロバイダーは複数のログフィードを生成します。あるものは運用メトリックスであり、あるものはセキュリティ指向であり、他のものはそれらの混合です。この文書では、セキュリティログに焦点を当てます。

フェーズ 1 では、スタートアップ企業は IaaS/PaaS プロバイダーの主なログフィードを有効にし、主にフォレンジック目的で中央ストレージに集めます。この時点では、通常、人員不足、成熟度、予算の制約のため、リアルタイムの分析は行われません。フェーズ2では、サービスが追加され、従業員が増加するにつれて、ログフィードが追加され、ログ収集および分析プラットフォームが実装されることが多くなります。フェーズ3では、スタートアップ企業は、定期的な脅威ハンティング手法を含め、すべての関連ログフィードを収集、分析、相関させる24時間365日のログモニタリングサービス（通常は外

部）で成熟させる必要があります。

210.3.1 セキュリティログ

セキュリティログと監査ログは、コンソールまたはAPIコールでクラウド構成の変更を記録する、デジタル証跡として機能します。例えば、AWS CloudTrail、Azure Activity Log、Google Cloud Audit Logsなどです。これらのログは、トラブルシューティング、コンプライアンス、セキュリティ、フォレンジック分析に不可欠です。スタートアップ企業は、最初からすべての関連地域でこれらのログフィードを有効にし、中央の場所（例えばデータレイク）にそれらをルーティングする必要があります。ログは成熟するにつれて追加され、より詳細な分析、相関、モニタリングが適用されます。

210.3.2 トラフィックログ

これらのログは、特定のVPC/VNET内のネットワークインターフェースを出入りするIPトラフィックに関する情報を取得します。トラフィックログは、送信元と宛先のIPアドレス、ポート、プロトコル、パケット数（フロー形式）などのネットワークトラフィックパターンを可視化します。ネットワークモニタリング、セキュリティ分析、およびコンプライアンス監査に役立ちます。例としては、GCPおよびAWS VPCのフローログとAzure VNETのフローログがあります。デフォルトでは、クラウドプロバイダーはテナントのトラフィックのログを収集して提示することはありません。
利用者は、関連するvpc/vnetでロギングサービスを有効にすることで、トラフィックログを有効にする必要があります。トラフィックログは大規模なデプロイメントではコストがかかるため、有効化は本番環境に限定されることがよくあります。

210.3.3 クラウドサービスログ

ほとんどのクラウドサービスは、主にパフォーマンスのモニタリングとテレメトリの収集を目的として運用ログを提供していますが、これらのログは貴重なセキュリティ上の洞察を生成し、フォレンジック分析を支援することもできます。
パフォーマンスメトリクスとアプリケーションデータをログに統合することで、リソースの健全性と全体的な運用効率を可視化できます。

210.3.4 ワークロードログ

ワークロードとは、実際の計算を実行する仮想マシン、コンテナ、サーバーレス機能のことです。各ワークロードは、オペレーティングシステムに基づいてログを生成します。Windowsワークロードは Windowsイベントビューアを生成し、Linuxはsyslog形式でログを報告します。コンテナとKubernetes は、独自のランタイムと設定ログを生成します。重要なワークロードからセキュリティ関連のログを収

集、分析、保存することは、標準的なセキュリティのベストプラクティスです。ワークロードからこれらのログを収集し、一元化するためのツールは、商用およびオープンソースで複数あります。

マネージメントプレーン・ログ	サービス・ログ	リソース・ログ	クラウド・ツール
マネージメントプレーンの保護の重要性が指摘されたクリティカルな情報源	• APIゲートウェイ：アクセスログ • ストレージ：アクセスログ • ネットワーク：VPC Flowログ • ファンクション/サーバーレス：アクティビティログ • クラウド・ロードバランサ：アクティビティログ • クラウドDNS:クエリログ • クラウドWAF/ファイアウォール：アクティビティログ	• ワークロード：インスタンス、VMログ • 構成変更ログ • クラウドFunction Invocationログ • データベース・トランザクションログ • オブジェクトストレージファイル・アクセスログ • スナップショットとイメージログ（ブロックストレージ）	• CSPM(Cloud Security Posture Management - SPM) • CASB(Cloud Access Security Broker) • CNAPP(Cloud Native Application Protection Platform) • SSPM(SaaS SPM) • DSPM(Data SPM) • IAM Analytics • CDR(Cloud Detection and Response)

図2:クラウドテレメトリーソース

2.10.4 SIEM、データレイク、クラウドの検知と対応

2.10.4.1 SIEM (Security Information and Event Management)

このシステムは、様々なリソースからログを収集・統合し、事前定義された設定によって相関関係を見つけることができるセキュリティソリューションです（ログソースは、上記のセクションのログタイプのいずれかになります）。たとえば、ワークロードを実行したり、ネットワーク構成を変更したりするための特定の役割を持つ新しいユーザーが作成された場合に、アラートを発生させるルールを作成できます。SIEM は、セキュリティインシデントの特定と対応、セキュリティイベントの分析、および法規制コンプライアンスの確保によって、クラウド環境におけるセキュリティの可視性を高めます。Azure SentinelやGoogle ChronicleはクラウドSIEMの一例です。その他の選択肢としては、Splunk、Arcsight、IBMなどがあります。

2.10.4.2 SDL（セキュリティデータレイク）

データレイクとは、膨大な量の構造化・非構造化データを生のままクラウド上に保存する一元的なリポ

ジトリのことです。その目的は、ビッグデータ分析、機械学習、アナリティクスのためのスケーラブルでコスト効率の高いストレージを実現することです。クラウドデータレイクの例としては、AWS Security Lake、Amazon Security Lake、ELK（Elastic、Log stash、Kibana）などがあります。セキュリティデータレイクは、複数のフォーマットで膨大なデータを柔軟に集約し、簡単に分析できるようにすることで、SIEMツールを補完します。クラウドデータレイクは、クラウド環境内のさまざまなソースからログデータを収集し保存する上で非常に重要です。このデータは、脅威ハンティングやインシデント分析に利用できます。

2.10.4.3 CDR（Cloud Detection and Response）

このソリューションは、クラウドネイティブのセキュリティコントロール、API、およびテレメトリーデータを活用して、クラウドのワークロード、アプリケーション、およびユーザーのアクティビティをリアルタイムで可視化します。これにより、セキュリティチームは、クラウド環境における不審な行動の特定と調査、セキュリティポリシーの適用、脅威の効果的な修復を行うことができます。CDRは、クラウド環境向けのSIEMを進化させたものです。この記事が書かれている時点では、業界全体で統一された定義はなく、従来のSIEMとの関係についての意見もさまざまです。CDRソリューションの主な機能には、継続的なモニタリング、脅威の検出、インシデントレスポンスの自動化、セキュリティオーケストレーションおよび自動化ツールとの統合などがあります。

2.10.5 ロギング

フェーズ1では、ほとんどのスタートアップがクラウドプロバイダーの主要なポスチャーツール（AWS security hub/ Azure security center）と基本的なロギングオプション（管理証跡ログと一部の重要なサービス）を有効にし、それらを中央ストレージに収集します。重要なアラートは通常この段階でのみ扱われ、分析作業はまだ散発的でインシデントベースです。

フェーズ2では、より多くのログフィードが追加され（ネットワークログ、新規サービスが導入される）、効率的な収集と分析を行うには、セキュリティデータレイクを実装することが多くの場合、良い選択肢となります。現在、CSPMツールはすべてのIaaS/PaaS環境を基本的なモニタリングでカバーし、最も重要なログを収集・保存する必要があります。

フェーズ3では、成熟したモニタリング手順を提示する必要があります。マルチクラウドのスタートアップは、マルチクラウドをカバーするためにサードパーティのCSPMソリューションを採用し、重要なログやイベントは中央の場所に収集・保存されるか、クラウドプラットフォーム自体に分散されます。定期的な脅威ハンティングの手順が導入され、イベントモニタリングは通常、外部の第三者によって24時間365日行われるようになりました。

211 章のサマリー

	フェーズ1	フェーズ2	フェーズ3
アーキテクチャ	単一地域/マルチゾーン。基本的なポリシーを持つdev/prod用の複数アカウント。シンプルなIACテンプレート。	IACと自動化の成熟。影響範囲保護の成熟 - より多くのVPC/アカウント。 冗長性とバックアップは成熟しつつあります（基本的なDR機能）。	DRは成熟しています。マルチリージョン展開（ビジネスニーズによる） 影響範囲は、セグメンテーション、IAC、およびワークロード分離を導入することで最小限に抑えられます。 環境アクセス：JIT/PIMの使用。
データセキュリティ	データの所在地のマップ。あらゆる場所でTLSを強制します。暗号化ストレージポリシーを作成します。	データ分類手順の作成。 プロバイダーKMSを使用して複数の暗号化鍵を作成し、鍵に関する厳格なアドミニストレーター管理を行います。	顧客がBYOKを行えるようにします（該当する場合）。 自動検出、分類、およびガバナンスのためのデータセキュリティポスチャー管理の実装
IAM	IDPの実装。MFAとモダン認証の導入。ベーシック認可。手動オンボーディング	開発部門と本番運用部門の分離従業員のオンボード/オフボードの自動化。 サービスアカウントのマッピングと基本的なシークレットボールトの使用	きめ細かいカスタムロール。 臨時アクセスの使用。 管理者アカウントの特権アイデンティティ管理。成熟したシークレット管理。 サービスアカウントとシークレットの作成とローテーションの自動化
ワークロードセキュリティ	ハードニングされた信頼できるイメージと基本的な脆弱性スキャンを使用します。クラウドネイティブツールの使用	あらゆる種類のワークロード（コンテナを含む）におけるCWPP。 パッチは迅速にインストールされるようになります。	k8sのランタイムセキュリティと自動パッチ適用。 マルウェア対策（EDR/AV）は現状で成熟しています。

モニタリング	CSP内蔵のポスチャーツールから始めます。 管理プレーンのログを有効にし、中央の場所に集めることを確実にしてください。 所見の定期的な見直し	24時間365日のモニタリングは成熟しています。ログソースの追加（フローログ、ワークロード、サービス） 注意喚起の手順	自動対応プレイブック 定期的な脅威ハンティング。 成熟したCDRポリシー マルチクラウドのポスチャ管理（要件に基づく）

3. アプリケーションセキュリティ

3.1 SSDLCの紹介

セキュアソフトウェア開発ライフサイクル（SSDLC）は、ソフトウェア開発に対する積極的なアプローチを示すものであり、そこではセキュリティがすべての段階で基本的な考慮事項となります。スタートアップ企業にとってSSDLCの採用は、開発プロセスにセキュリティを組み込むことを意味します。SSDLCは、セキュリティを個別のフェーズや最終チェックとみなすのではなく、初期の計画段階から開発、配備、および保守に至るまで、セキュリティの実践を統合することを目指しています。この全体的なアプローチにより、セキュリティが後付けではなく、開発ライフサイクル全体を通じて継続的に重視されるようになります。

限られたリソースと迅速な開発サイクルにより、スタートアップ企業はサイバーセキュリティに関する独自の課題に直面しています。アプリケーションセキュリティ（AppSec）対策を早期に実施することは大変なことですが、重要であり、努力する価値があります。セキュリティコントロール、サービス、および製品の実装に関する意思決定は、特にセキュリティに強いバックグラウンドを持たないチームにとっては、不明確なままであることがよくあります。SSDLC に着手する前に、研究開発（R&D）チームは、セキュリティコントロールを統合する必要性、実装の程度、およびタイミングをより良く検証するために、以下の質問を検討する必要があります。

- 保護が必要な最も重要な資産（クラウンジュエル）は何ですか？
- 潜在的な脅威と脆弱性は何ですか（後述：脅威モデリング、アタックサーフェス）？
- セキュリティコントロールは、開発のどの段階（ステージ）で実施すべきですか？
- これらのコントロールの有効性をどのように測定すれば良いですか（そしてそれをどうすれば良いですか）？

3.1.1 意識向上とトレーニング

セキュリティ意識は、組織を守るために全社を巻き込む基礎的なものです。アプリケーションベースのインシデントが頻発するようになってきているため、アプリケーション関連の担当者、特に開発者がアプリケーションセキュリティに精通していることが不可欠です。

- **初期フェーズ**：開発者は、OWASP トップ 10やOWASP セキュア・コーディング・プラクティス・チェックリストのような、基本的なセキュリティの概念に慣れ親しむべきです。
- **成熟期フェーズ**：組織のセキュリティ意識向上プラットフォーム（KnowBe4、Phish.me、Wizer など）を拡張し、開発者に焦点を当てたプログラムを含めるようにします。
- **成長段階フェーズ**：PluralSight、Udemy、Coursera、Secure Code Warriorのような高度なセキュアコーディングの認識とトレーニングプラットフォームに投資します。これらのプラットフォー

ムは、技術トレーニングセッションや、Capture The Flag (Google CTFや Hack The Box)などのゲーミフィケーション要素を提供し、開発者の関心を高め、競争的な学習環境を育成します。

開発者の意識向上のためのコアコンセプト：

- **アタックサーフェス**：SQLインジェクションやクロスサイトスクリプティングなど、アプリケーションを標的とする可能性のある一般的な脆弱性についてチームを教育します。何をするにしても、セキュリティに影響を及ぼす可能性があることを理解させましょう（S3バケットを公開する、特権アクセスを持つサービスアカウントを利用する、など）。
- **脅威モデリング**：これは、潜在的な脅威と脆弱性を設計フェーズの早い段階で特定し、セキュリティ対策を開発プログラム／アーキテクチャに統合できるようにし、よりセキュアな設計のために開発チームとセキュリティチームの協力を促進するための構造化されたプロセスです。STRIDE、PASTA、DREADのようなフレームワークは、潜在的なリスクを体系的に評価し、軽減することで、このプロセスを簡素化することができます。
- **セキュリティ文化**：チーム全体にセキュリティを意識したマインドセットを醸成します。
- **セキュリティの実践とコーディング**：セキュアコーディング、およびDevSecや実用的な暗号などの関連概念に関する実践的なトレーニングを提供します。
- **応用的なセキュリティ基準と概念**：OWASP SAMM、OWASP ASVS、セキュリティ・ばい・デザインとプライバシー・バイ・デザインなどの主要なアプリケーションセキュリティ標準をチームに紹介します。
- **セキュアなアーキテクチャ**：セキュアなアーキテクチャ設計のベストプラクティスをチームに提供します。
- **データ保護**：転送中、保存中、および使用中のデータの暗号化（例：コンフィデンシャルコンピューティング）、パスワードのハッシュ化など、データ保護の原則をチームに理解させます。さらに、API鍵、パスワード、および証明書などの機密情報をセキュアに保管、管理、およびアクセスするための強固なシークレット管理手法を導入し、不正アクセスや露出のリスクを低減します。
- **フリー&オープンソースソフトウェア（FOSS）**：ライセンス、コンプライアンス、サードパーティコンポーネントのリスクなど、FOSSを利用する利点と課題についてチームを教育します。
- **セキュリティテストとツール**：セキュリティテストツール（SCA、SAST、DAST など）と、アプリケーションセキュリティの維持におけるその役割について、チームによく理解してもらいます。

3.1.2 セキュアな開発プラクティス

セキュアなアプリケーションを構築するには、設計から本番に至るまで、開発のあらゆる段階でセキュリティに取り組む必要があります。スタートアップ企業は、脆弱性を防止し、セキュリティを意識した開発文化の基盤を確立するために、できるだけ早い段階でセキュアなアーキテクチャの実践を組み込むべきです。

- **フェーズ1（インセプション）**：入力と出力の検証、暗号化（転送中と保存中の両方）、シークレットマネージャを使用した適切なシークレット管理（コードそのものの内部ではなく）、適切なアイデンティティとアクセス管理の実装（主に強固な認証（MFA を含む）、適切な認可（ロールと、そのロールが作成、読み取り、更新、削除（CRUD）できるもの）、説明責任（ログイン、ログアウト、および、他の機密トランザクションのログを記録）、チーム内のセキュアなコーディング文化の確立（ピアによるコードレビューを含む）、オープンソースライブラリのセキュリティパッチ（SCA）。
- **フェーズ2（成熟期）**：アタックサーフェスを理解する、OWASP Top 10 に従う、設計と開発初期段階においてセキュリティが重要な考慮事項であることを確認する、静的アプリケーションセキュリティテスト（SAST）を実施する、開発プラットフォーム（IDE）に組み込むなどのフレームワークを導入することによって、フェーズ 1 のプラクティスを拡張します 。
- **フェーズ3（成長段階）**：脅威モデリング、OWASP SAMM、Security and Privacy by Design and Default（設計とデフォルトによるセキュリティとプライバシー）、より洗練された技法（動的アプリケーションセキュリティテスト（DAST）、あるいは、より良い方法として、対話型アプリケーションセキュリティテスト（IAST））のような、より高度なプラクティスを統合することによって、セキュリティ対策を強化します。

キーコンセプト：

- **入力検証と出力エンコード**：SQLインジェクションやクロスサイトスクリプティングのような一般的な攻撃を防ぐために、すべてのユーザー入力が検証され、サニタイズされていることを確認します。
- **認証と認可**：強力な認証（AuthN）と認可（AuthZ）メカニズムの設計と実装。このような機密性の高いコンポーネントの処理には、確立されたデザインパターンやサードパーティのサービスを利用することを検討してください。
- **暗号化**：強固な暗号化アルゴリズムとセキュアな鍵管理手法で機密データを保護します。
- **効果的なロギングとモニタリング**：セキュリティインシデントを検出し対応するために、包括的なロギングとモニタリングを実施します。
- **エラー処理**：機密情報の漏洩を防ぐためには、セキュアなエラー処理を行うことが重要です。

3.1.3 セキュリティ保証とテスト

設計と実装が完了したら、次のステップでは、さまざまなテストツールとテクニックを活用して、高いセキュリティ保証を確実にします。包括的な AppSec テストプログラムは、複数の方法を組み合わせて最高のカバレッジを達成する必要があります。3.1.2では、このリストが成熟度フェーズとともに示されています。

テストの実践：

- **コードレビュー（CR）**：プルリクエスト(PR)の各段階でセキュアなコードレビューを定期的に実施します。
- **ソフトウェア構成分析 (SCA):**SCAツールはオープンソースのコンポーネントを管理し、サードパーティのコードに関連するリスクを軽減します。
- **静的アプリケーションセキュリティテスト (SAST):**SASTツールは、開発の初期段階でソースコードの脆弱性を特定するために役立ちます。
- **動的アプリケーションセキュリティテスト (DAST):**DASTツールは、実行中のアプリケーションの脆弱性を特定するための侵入テストをシミュレートします。
- **会話的アプリケーションセキュリティテスト（IAST）**は、静的分析と動的分析を組み合わせて、潜在的なセキュリティ課題を包括的に示します。
- **ペネトレーションテスト(PT):**定期的な侵入テストは、社内で実施するか第三者の専門家に依頼するかを問わず、脆弱性を特定し対処するために不可欠です。

助言：オープンソースのツールを活用することで、アプリケーションセキュリティスキャンの成熟プロセスを簡素化することができます。いくつか例を挙げます。
Automated-Security-Helper- コードのスキャン、脆弱性の検出、シークレットの留置のための複数のオープンソースパッケージを統合します、
Zed Attack Proxy (ZAP)- OWASP ZAP は、ウェブアプリケーションの脆弱性を発見するためのオープンソースのDASTツールです。
GitHub—aqua security/trivia: コンテナ、Kubernetes、コードリポジトリ、クラウドなどの脆弱性、設定ミス、シークレット、およびSBOMを検索し、コード内の脆弱性、設定ミス、およびシークレットを見つけます。

3.1.4 アプリケーションセキュリティメトリクス

アプリケーションセキュリティメトリクスは、アプリケーションのセキュリティ、有効性、および成熟度を評価するための定量化可能な測定基準をスタートアップ企業に提供します。これらの指標を統合することで、スタートアップ企業はリスクレベルを評価し、改善努力の優先順位を付け、セキュリティコントロールの実施状況を監視することができます。

主な指標：

- **脆弱性密度（Vulnerability Density）**は、特定のコードユニット内で特定された脆弱性の数を測定します。
- **セキュリティテストカバレッジ（Security Testing Coverage）**は、アプリケーションがセキュリティテスト活動を受けた程度を評価します。
- **コード品質（Code Quality）**は、セキュリティの観点からコードの品質を評価します。
- **セキュリティパッチ適用（Security Patching Cadence）**は、セキュリティパッチやアップデートがアプリケーションに適用されるスピードを追跡します。
- 平均検出/解決時間（Mean Time To Detect/Resolve）は、セキュリティインシデントを特定また

は解決するまでの平均時間を測定します。
- **コンプライアンス遵守**（Compliance Adherence）は、組織が関連するセキュリティ標準や規制に準拠しているかを評価します。
- **セキュリティ意識向上**（Security Awareness）は、修了率やフィッシングテストの頻度など、セキュリティトレーニングプログラムの効果を測定します。

3.2 ソフトウェアサプライチェーンセキュリティ

サイバーセキュリティにおけるサプライチェーンセキュリティとは、組織のサプライヤー、プロバイダー、パートナー（在庫管理システム、調達プラットフォーム、ロジスティクスソフトウェア、その他のテクノロジーなど）をセキュアに管理する手法を指します。この章では、ソフトウェアの開発サイクルの中で、私たちが使用したり、利用したりする複数の外部コンポーネントをセキュアにする方法について、ソフトウェアのサプライチェーンのセキュリティに焦点を当てます。

ソフトウェアサプライチェーンの課題
開発者は、開発を加速させ、専門知識を活用するために、サードパーティのソフトウェアコンポーネントを使用するのが一般的です。

例えば、以下のようなものです。

- コードスニペット
- オープンソース/クローズドソースライブラリ
- サードパーティAPI
- クラウドサービス

このような依存関係は、製品ライフサイクル全体を通して評価・管理されなければならないリスクをもたらします。

リスクカテゴリーには以下のものが含まれます（非網羅的リスト）。

- サードパーティ製コンポーネントの脆弱性
- 一般公開されているライブラリに含まれる悪意のあるコード
- 互換性のリスク
- サポートリスク
- 知財およびライセンスリスク

以下の段落では、ソフトウェアのサプライチェーンとセキュリティのリスク管理を支援するためにデプロイされる可能性のあるツールやプロセスの概要と、スタートアップ企業のライフサイクルの各カテゴリーにおけるリスク管理の実施に関する推奨事項を説明します。

3.2.1 オープンソースガバナンスの推奨

オープンソースソフトウェアとは、ソースコードが一般に公開され、誰でもソースコードを検査、修正、および拡張したり、あるいは変更を加えることなく第三者のコンポーネントをそのまま利用したりすることができるソフトウェアです。この協調的なアプローチにより、多様な開発者コミュニティがソフトウェアに貢献し、改善することが可能になり、イノベーション、透明性、および迅速な問題解決が促進されます。オープンソースプロジェクトは、ユーザーが自由にソフトウェアを使用、変更、および配布することを許可するライセンスの下で配布されることが多く、MIT、Apache 2.0、GNU General Public License (GPL)などの一般的なライセンスがあります。オープンソースモデルは、現代のソフトウェア開発の礎石となり、技術の進歩を促進し、世界中の個人や組織にアクセス可能なソリューションを提供しています。
しかし、オープンソースのスタートアップ企業は、対処すべき複数のリスクにさらされています。主なリスクは以下の通りです。

- **セキュリティの脆弱性**は、オープンソースコードと同様、一般に公開されており、適切に保守・監視されなければエクスプロイトされる可能性があります。
- **ライセンスコンプライアンス**。（GPLのような）制限のあるライセンスでOSSを使用すると、スタートアップ企業のプロプライエタリなコードに法的義務が課される可能性があります。
- **コミュニティが支援するプロジェクトに依存**すると、プロジェクトが放棄されたり、タイムリーな更新が行われなかったりするため、安定性やサポートに課題が生じる可能性があります。
- **オープンソースのコンポーネントを統合**すると、互換性や統合の課題が発生し、開発が遅れたり、技術的負債が生じたりする可能性があります。

以下は、スタートアップ企業のライフタイム段階におけるこれらのリスクを管理するための推奨事項です。

フェーズ1（インセプション）では、以下の活動を行います。

- 役割と責任を含め、オープンソース利用の基本方針を作成します。CTOまたはR&D VPは、オープンソースの使用を事前に承認する必要があります。
- 技術的ニーズやコア機能の実装を支援するオープンソースプロジェクトを調査・評価します。
- 定評のあるオープンソースプロジェクトの利用を優先します。
- オープンソースライセンスを理解し、法的課題を回避するためのコンプライアンスを確保します。

フェーズ2（成熟期）では、以下の活動を行います。

- 定期的なスキャンとアップデートを実施し、脆弱性を軽減します。
- オープンソースソリューションのパフォーマンスとスケーラビリティを継続的に評価します。
- オープンソースツールを最適化し、顧客のニーズに合わせてカスタマイズします（カスタマイズによっては、スタートアップ企業がより多くのメンテナンス責任を負う必要がある場合があ

ることに注意してください）。
- 継続的インテグレーションと継続的デプロイメント（CI/CD）手順に統合されたソフトウェア構成分析（SCA）やソフトウェア部品表（SBOM）などのツールを活用して、より高度なガバナンスポリシーを導入します。

フェーズ3（成長段階）では、以下の活動を行います。

- オープンソースへの戦略的アプローチを開発し、利用と貢献のバランスをとります。
- 利用するオープンソースプロジェクトの持続可能性を確実にします。
- オープンソース技術の革新と利用拡大を継続します。
- オープンソースプロジェクトを公開することで、人材を集め、信頼性を高めることを検討します。
- サイバー脅威インテリジェンス（CTI）を使用して、使用されているオープンソースプロジェクトに関連する侵害や漏えいを警告します。

3.2.2 クローズドソースのサードパーティライブラリ

クローズドソースのライブラリは、オープンソースと同様のリスクをもたらすため、スタートアップ企業のライフサイクル全体を通して同じように注意深く管理されるべきです。

可能であれば、SCAとSBOMのプロセスに組み込んでください。SCAツールでカバーできない場合は、別のリスク管理戦略を実施すべきです。

3.2.3 サードパーティAPI

サードパーティAPIの呼び出しは、情報強化や検索のようなタスクのための標準的なものです。クローズドソースソフトウェアとリスクを共有し、さらなる懸念をもたらします。

- **可用性**：ネットワークアクセスとプロバイダーの信頼性への依存。
- **MITM攻撃**：通信傍受に対する脆弱性。
- **プロバイダーの侵害**：API プロバイダーまたはそのサブサプライヤに対するサイバー攻撃。
- **IP/データ漏洩**：知的財産や顧客データの誤った取り扱いの可能性。

スタートアップ企業のフェーズ2では、サードパーティリスク管理（TPRM）プロセスの一環として、スタートアップ企業はこれらのリスクを管理する必要があります。

3.3 ソフトウェアの変更管理

ソフトウェア変更管理とは、ソフトウェアアプリケーションやシステムの変更を管理および実施することです。その目標は、ソフトウェアの品質、完全性、およびセキュリティを維持しながら、最小限の途絶で効率的に変更が行われるようにすることです。このプロセスには、変更要求を処理し、その影響を評価し、すべての段階でセキュリティへの配慮を取り入れながら、コントロールされた方法で変更要求を実施するための重要なステップがいくつかあります。

以下は、ソフトウェア変更管理の主なステップです。

3.3.1 変更要求

変更を追跡し、ソフトウェアのバージョンを管理し、ソフトウェアに導入された課題の根本原因を特定できるように、すべての変更は変更要求として文書化されなければなりません。
変更要求は、正式な変更要求フォーム、製品管理ユーザーストーリー、カスタマーサポートリクエスト、PR記述、チケットシステム、またはその他の永続的で検索可能な方法で文書化することができます。

ホットフィックスとは、システム障害や特定された重大な脆弱性、バグにより直ちに必要となる変更であり、ソーシャルメディアや電子メールなどの即時のコミュニケーション手段を通じて一時的に文書化することができますが、適用後も同様に文書化する必要があります。

3.3.2 承認と優先順位付け

すべての変更は、技術、運用、ビジネス、およびセキュリティへの影響やリスクを含め、既存のソフトウェアへの影響を評価する必要があります。

変更の承認には、影響とリスクの管理、および変更実施の優先順位付けが含まれなければなりません。

セキュリティレビューは、いかなる承認決定にも含まれなければなりません。変更の種類や優先順位（営業時間外のホットフィックスを誰が承認できるかなど）を考慮して、承認権限を設定する必要があります。

3.3.3 計画とスケジューリング

承認後、ソフトウェア、データベース、インフラストラクチャ、構成、およびセキュリティコントロール要件など、各変更を計画する必要があります。

変更計画には、スケジュール、リソースの割り当て、テスト戦略、セキュリティ対策、およびロールバック計画を含める必要があります。

3.3.4 実装

計画通りに変更を開発し、構成します。実施中にスコープ、リスク、または要件が大幅に変更された場合は、承認と優先順位付けのステップをやり直すべきかどうかを評価します。

計画されたテスト戦略に従って、包括的なテストを実施します。セキュアなデプロイプラクティスを使用して変更を本番環境にデプロイします。可能な限りデプロイメントを自動化します。

3.3.5 実施後のタスク

1. 変更実施後の検証とレビューの実施。
2. コードベース、設定ファイル、マニュアル、およびセキュリティポリシーや手順など、関連するすべてのドキュメントを更新します。
3. ユーザー、顧客、サポートチーム、およびセキュリティチームなど、関連するすべての利害関係者に変更を伝達します。
4. 変更の有効性を長期にわたって監視し、有効性を確保するとともに、生じる課題を特定します。
5. 変更に関する関係者へのトレーニングを実施し、トレーニング資料を適宜更新します。
6. 実装後のレビューを実施し、教訓をフィードバックし、変更管理とセキュリティプロセスを改善します。

以下は、スタートアップ企業のライフタイムのフェーズにおけるこれらのリスクを管理するための推奨事項です。

フェーズ1（インセプション）では、以下の活動を行います。

1. 変更要求と承認を文書化するためのシンプルで明確なプロセスを導入します。
2. ソースコントロールやチケットシステムなど、変更をコントロール・追跡するための基本的なツールを使用します。
3. 明確な役割と責任を定め、チームメンバーに変更管理のトレーニングを提供します。
4. 変更要求プロセスにおける基本的なセキュリティレビューを実施します。

フェーズ2（成熟期）では、以下の活動を行います。

1. 脆弱性を軽減するために、すべてのソフトウェアコンポーネントを定期的に更新し、パッチを適用します。

2. 変更管理のための詳細な標準作業手順書（SOP）を作成します。
3. より高度なツール（CI/CDパイプラインなど）を使って変更管理プロセスを自動化します。
4. 包括的なセキュリティテストを変更管理プロセスに統合します。
5. すべての重要な変更について詳細なリスク評価を実施します。

フェーズ3（成長段階）では、以下の活動を行います。

1. 変更マネージャーやセキュリティオフィサーなど、専任の役割を導入します。
2. エンタープライズグレードの変更管理ツールを導入します。
3. 変更管理プロセスを他のITおよびビジネスプロセスと完全に統合します。
4. 業界の規制や基準を遵守するための強固なガバナンスの枠組みを構築します。

3.4 CI/CD セキュリティと Infrastructure as Code

継続的インテグレーション/継続的デプロイメント（CI/CD）、Infrastructure as Code（IaC）、Policy as Code（PaC）は、現代のソフトウェア開発、特にSaaSベースのスタートアップ企業にとって重要なアプローチです。CI/CDはコード変更のビルド、テスト、およびデプロイを自動化し、IaCはコードと自動化を使用してインフラストラクチャーリソースを管理し、PaCはIaCのガードレールとして機能します。これらのアプローチは効率性と一貫性を向上させ、セキュリティの強化に不可欠です。

CI/CD パイプラインへのセキュリティの組み込み

- 開発ライフサイクルの早い段階でセキュリティを統合する「シフトレフト」アプローチを採用します。
- 自動化されたセキュリティテスト（Secret Scanning、SAST、DAST、Container Scanning）を CI/CD パイプラインに組み込みます。
- 依存関係、ライブラリ、およびサードパーティ製コンポーネントの脆弱性を定期的にスキャンします。これにより、セキュリティ上の欠陥がエクスプロイトされる前に修正できます。
- 使用されるすべてのサードパーティ製コンポーネントを文書化するためにSBOMを追加します。

IaCによるセキュリティ強化

- セキュリティ・バイ・デザインを採用し、デフォルトでセキュリティポリシーとコンプライアンス要件をコードコンポーネントとして組み込みます。例えば、アクセス制御や暗号化の設定をコードとして定義することができます。
- バージョンコントロール：IaCおよびPaCテンプレートはバージョン化され、ソースコードリポジトリに保存できるため、追跡、監査、および課題発生時の迅速なリカバリが可能です。

- 一貫性、再現性、スケーラビリティ：IaCは、インフラストラクチャが異なる環境間で一貫性を

維持することを確実にし、設定のドリフトや手動設定による脆弱性を低減し、スケーリングプロセスを簡素化します。

- コンプライアンス：IaC は、セキュアな設定テンプレートの作成、監査証跡の提供、自動コンプライアンススキャンの有効化、および必要なコンプライアンス更新の自動実行を可能にすることで、コンプライアンスを大幅に促進します。

これらのプラクティスの導入は、スタートアップの成熟度に応じた段階的なアプローチに従うべきです。

フェーズ1:
すべてのコードとインフラストラクチャ定義の基本的なバージョンコントロールを実装します。最小限の自動テストでシンプルなCIパイプラインを確立します。CI/CDシステムの基本的なアクセス制御を設定します。コアインフラストラクチャーコンポーネントのシンプルなIaCテンプレートの使用を開始します。重要なコンポーネントの手動コードレビューを実施します。

フェーズ2:
主に静的アプリケーションセキュリティテスト（SAST）を中心とした、自動化されたセキュリティテストで CI/CD パイプラインを強化します。依存関係やサードパーティコンポーネントの脆弱性スキャンを実施します。コードとしての基本的なセキュリティポリシーを含め、IaCの使用を拡大します。IaCテンプレートのバージョンコントロールを実装します。セキュリティの知識と基本的なツールを開発者に紹介することから、シフトレフトを始めましょう。

フェーズ3:
SAST、DAST、コンテナスキャン、Function-as-a-Serviceスキャンを含む、CI/CDにおける高度な自動セキュリティテストによる包括的な「シフトレフト」アプローチを導入します。包括的なセキュリティポリシーとコンプライアンス要件をコードとして組み込み、すべてのインフラストラクチャにIaCを完全に導入します。
IaCによる高度なアクセス制御と暗号化設定の実装。CI/CDパイプライン内で自動化されたコンプライアンススキャンを確立します。IaCを使用することで、環境間で完全な一貫性と再現性を確保することができます。IaCプラクティスにおける自動セキュリティテストとコンプライアンス更新を実装します。

3.5 API管理とウエブアプリケーションファイアウォール (WAF)

API管理とウエブアプリケーションファイアウォール（WAF）は、SaaSベースのスタートアップ企業にとって、WebアプリケーションとAPIをセキュアにする上で非常に重要です。WAFは、WebアプリケーションとインターネットHTTPトラフィックをフィルタリングして監視し、一般的な攻撃から保護します。適切なAPI管理は、SaaSビジネスにとって重要なAPIのセキュアかつ効率的な取り扱いを確実にします。

WAFは必須ではありませんが、SaaSプロバイダーを評価する際に、その存在について問い合わせる企業顧客は少なくありません。

フェーズ 1:
初期段階では、基本的なセキュリティ対策の実施に重点を置いてください。利用が限定的なAPIや、本番システムへの影響が最小限のAPIについては、ゲートウェイを使用しない直接のAPI管理で十分な場合があります。APIの基本的な認証と認可を実装し、将来の分析のためにAPIコールのログを開始します。パブリックなAPIやよりクリティカルなAPIを扱う場合は、許可リスト/ブロックリストやレート制限機能を含む基本的な管理のために、クラウドプロバイダーのAPI Gatewayを使用することを検討してください。ウェブアプリケーションの保護については、ホスティングプラットフォームやウェブサーバーが提供するセキュリ ティ機能から始めてください。

フェーズ 2:
スタートアップ企業が成熟し、APIの利用が増加するにつれて、トラフィック量、セキュリティ要件、スロットリングや詳細な分析のような機能に基づいてAPIゲートウェイの必要性を評価します。実装されている場合は、APIのバージョニングやきめ細かなアクセス制御など、より高度な機能でAPIゲートウェイの利用を強化します。ウェブアプリケーションセキュリティについては、基本的なWAFを実装し、多くの場合はクラウドプロバイダーの組み込みサービスを利用します。APIの使用パターンのモニタリングを開始し、基本的な異常検知を実装します。APIゲートウェイを使用しない場合、これらのセキュリティ対策がアプリケーションレベルで実装されているか、他のセキュリティツールによって実装されていることを確認してください。

フェーズ 3:
このフェーズでは、従来のAPIゲートウェイ機能を超えた、包括的なAPIセキュリティプラットフォームを実装します。このプラットフォームには高度なAPIディスカバリ機能が含まれている必要があり、シャドーAPIや忘れられたAPIを含め、環境内のすべてのAPIの自動検出とインベントリを可能にします。APIのセキュリティ状況をよりよく理解するために、APIポスチャ管理を導入してください。これには、APIエコシステム全体にわたるAPI設定、アクセス制御、および使用パターンの継続的なモニタリングが含まれます。このプラットフォームは、高度な分析、リアルタイムの脅威検出、およびAPIの動作に特化した異常識別を提供する必要があります。Web アプリケーションのセキュリティについては、特定のニーズに合わせた機能を備えた高度な、場合によってはサードパーティのWAFソリューションを導入してください。重大な脅威に直面している場合は、専用のDDoS保護を検討してください。すべてのWebアプリケーションとAPIの継続的なセキュリティテストとモニタリングを確立します。この成熟したアプローチは、既知のAPIの管理と、未知のAPIまたは管理されていないAPIの検出と保護を確実にし、APIランドスケープ全体に包括的なセキュリティポスチャを提供します。

> 助言：多くのSaaSベースのスタートアップ企業は、マネージドWAFとDDOS保護を使用しています。Akamai、Cloud Flare、Incapsula などのベンダーは、CDN、DNS 管理、セキュアソケットレイヤー（SSL）証明書の自動更新、Zero-Trust アクセスなど、セキュリティ以外の複数の機能を備えたコスト効率の高いサービスを提供しています。

3.6 章のサマリー

	フェーズ1	フェーズ2	フェーズ3
SSDLC	基本的なセキュア開発プラクティス（例：入出力検証、基本的なセキュリ ティトレーニング、オープンソースライブラリのセキュリティパッチ適用）の実施。	アタックサーフェスを特定し、OWASP Top 10に準拠し、転送中および保存中のデータを暗号化することで、セキュリティ対策を拡大します。	セキュリティをすべての段階に完全に統合し、高度なセキュリティプラクティス、包括的な脅威モデリング、およびOWASP SAMMを導入します。
サプライチェーン	オープンソースライセンスの理解。 オープンソースの使用ポリシーを作成します。 既知の、評判の高いオープンソースライブラリを優先します。	サードパーティ製コンポーネントとその依存関係を定期的に更新します。 SCAとSBOMツールを使用してオープンソースの使用法と脆弱性を理解し、サードパーティのクローズドソースライブラリとAPIのリスクを管理します。	戦略的なSWサプライチェーン利用フレームワークを構築します。 CTIを適用して、サプライチェーンの脆弱性や侵害に関するアラートを受け取ることができます。 IP/データ漏洩に対する保護
変更管理	レビュー、リスク評価、および変更の承認を文書化します。ソースコントロールシステムとチケットシステムを使用して変更を追跡します。	SWアップデートとパッチを自動化します。 CI/CDパイプラインにおける変更管理を自動化します。 重要な変更に対する詳細なリスク評価を実施します。	変更管理専用の役割と責任を設定します。 エンタープライズグレードの変更管理ツールを導入します。変更管理をビジネスおよびITプロセスに統合します。
CD/CD & IAC	基本的なバージョンコントロールと簡単なCIパイプラインを実装します。コアコンポーネントにIaC PaCの使用を開始し、手作業によるコードレビューを実施します。	SASTと脆弱性スキャンによるCI/CDを強化します。コードとしての基本的なセキュリティポリシーなど、IaCの利用を拡大します。	高度な自動セキュリティテストによる包括的な「シフトレフト」を実施します。組み込まれたセキュリティポリシー、自動化されたコンプライアンススキャン、および一貫した環境管理により、IaCを完全に受け入れます。

API 管理とウエブアプリケーションファイアウォール (WAF)	基本的なAPIセキュリティの実装：認証、認可、ロギング 公開APIについては、基本的な管理機能を備えたクラウドAPI Gatewayを検討してください。 ホスティングプラットフォームのセキュリティ機能を活用してWebアプリケーションを保護します。	トラフィックとセキュリティの必要性に基づいてAPI Gatewayの必要性を評価します。 APIのバージョン管理、きめ細かなアクセス制御、および異常検知を実装します。 基本的なWAFを導入し、APIの使用状況を監視して異常なパターンがないか調べます。	APIディスカバリ、ポスチャ管理、およびリアルタイムの脅威検出を備えた高度なAPIセキュリティプラットフォームを採用します。 カスタマイズされた機能を備えたサードパーティ製WAFを導入し、DDoS防御を検討します。すべてのWebアプリケーションとAPIにおいて、継続的なセキュリティテストとモニタリングを実施します。

4. ガバナンス、リスク、コンプライアンス

4.1 リスク管理

4.1.1 はじめに

リスク管理は、セキュリティフレームワークの重要な要素です。SaaSのスタートアップ企業にとっては、複数の業界標準や規制を遵守しながら、潜在的なリスクを特定、評価、および対応する包括的なプロセスが必要です。

リスク管理とは、リスクの影響を許容範囲内に抑え、事業運営への支障を最小限に抑えるために、費用対効果の高いリスク管理を行うことです。SaaSベースのスタートアップ企業のリスク管理プロセスは、以下の点で異なります。

- 最初のうちは、スタートアップ企業はビジネスの優位性を得るために、より多くのリスクを取ります。このような場合、スタートアップ企業はこれらのリスクを軽減し、管理するために適切なコントロールを実施する必要があります。成熟すれば、そのプロセスも変わってきます。
- SaaSベースのスタートアップ企業は、顧客の信頼を得るために、コントロールと防御プロセスを透明化する必要があります。
- スタートアップ企業は、会社のコンプライアンス要件の一環として、リスク管理に関する意思決定を全面的に監査することが期待されています。
- スタートアップ企業は、自社のリスクだけでなく、顧客のリスクも考慮する必要があります。
- スタートアップ企業は、複数の職種や業務において第三者に大きく依存しており、サプライチェーンのリスク管理が必須となっています。

助言：リスク管理は継続的なプロセスです。時間の経過とともに企業が成長すれば、リスク許容度に応じて緩和策を調整および修正することが一般的です。しかし、リスクマネジメントプロセスが適切に行われれば、どのような脅威や脆弱性が組織に適用されるかを理解し、潜在的な脅威や影響に基づいて情報セキュリティ対策に優先順位を付け、リスクマネジメント活動を経営幹部に伝達し、企業の残存リスクを認識することができます。

4.1.2 資産

有形および無形資産とは、組織にとって価値のあるものを指します。これらの情報は、ビジネス上の価値、重要性、機密性、または財務的価値に従って分類されるべきです。組織は、リスク管理を目的として、すべての資産のインベントリを作成し、維持する必要があります。資産が特定されない場合、資産の追跡や適切な保護ができない可能性があります。スタートアップ企業の最初の段階では、資産リストは短く、手作業で行うことができます。成長に伴い、より自動化されたアプローチを検討する必要があります。

助言：スタートアップ企業の資産評価における良い出発点は、損失シナリオに焦点を当てることでしょう。これらの資産が完全に破壊された場合、どのような結果になるのでしょうか？

4.1.3 脅威

脅威は、組織の目的達成能力に悪影響を及ぼします。脅威には外部的なものと内部的なもの、意図的なものと意図的でないものがあります。組織は、ビジネス環境に適用される脅威を特定する必要があります。現代のクラウドベースのスタートアップ企業にとっての脅威のほとんどは、物理的なものよりもむしろデジタル関連のものでしょう。外部のサプライヤーや請負業者は、社内システムにアクセスできることが多く、潜在的な脅威として見過ごせません。

新しい技術が常に進化している中、企業は効果的なリスク管理を行うために、新たな脅威の最新情報を常に入手する必要があります。

助言：Cloud Security AllianceのTop Threatsワーキンググループは、クラウドの脅威と懸念をマッピングしています：
Top Cloud Threats | CSA

NIST has more general guidelines here:
NIST SP 800-12:Chapter 4 - Common Threats = A Brief Overview

4.1.4 リスク

リスクとは主に、ある事象が発生する確率と、それが組織に与える影響の組み合わせとして定義されます。イベントが成功する確率は、脆弱性をエクスプロイトする脅威エージェントの能力に依存します。

イベントの影響は、ビジネスインパクト分析（BIA）プロセスを通じて評価されることが理想的です。このプロセスでは、組織は、事業活動、資産、プロセスなどの重要性と、中断が発生した場合の影響を評価します。潜在的な結果を理解するためには、影響を見極めることが不可欠です。SaaSベースのスタートアップ企業の場合は、スタートアップ企業への直接的な影響だけでなく、顧客への潜在的な損害や組織の評判へのダメージも含める必要があります。

ほとんどの場合、組織はリスクを排除することはできませんが、許容可能なレベルまで軽減することができます。許容できるリスクのレベルは、経営幹部が決定しなければなりません。

リスクは動的なものであり、新たな脅威、攻撃、および脆弱性の進化に伴い、時間の経過とともに変化します。

4.1.4.1 AI関連リスク

人工知能（AI）技術の利用が加速する中、情報セキュリティリスクに関する新たな考慮事項が導入されています。これらのリスクの多くはよく知られているものですが、AIの要素が加わると複雑さが増し、企業は企業内での使用状況やビジネス環境に応じてこれらのリスクを評価する必要があります。出発点としては、社内外の潜在的な脅威要因に目を向けることでしょう。

外部の攻撃者は、（DeepfakeやLarge Language Model（LLM）などの）AI技術を活用し、より大規模で品質が向上した、より高度な攻撃を実行するでしょう。これらのリスクを軽減するために、Open Web Application Security Project のOWASP Top 10 for Large Language Model Applicationsを参照することが推奨されます。こうした敵対者に対する既存のコントロールを評価する際には、この変化を考慮しなければなりません。

一方、内部的な脅威は、ほとんどが生成AIツールの使用に関連しています。これらは、データ漏洩や、十分な検証なしに生成されたコンテンツに過度に依存するなどのリスクをもたらします。組織内でのAIツールやモデルの未認可な使用は、シャドーAI（不正AI）とも呼ばれています。組織は、これらのツールの使用を社内でモニタリングおよびコントロールし、未認可なデータの露出や検証されていないコンテンツの重要なプロセスへの組み込みに関連する潜在的な影響を軽減するために、警戒する必要があります。

現在のところ、AIに関わるリスクを効果的に軽減することは、スタートアップ企業にとって非常に複雑なことです。最初の措置として、AIの責任ある使用に関するガイドラインを定めた方針を策定し、従業員に配布し、さらにこのテーマに関する対話型のトレーニングセッションを実施します。このアプローチは、組織内でAI利用をめぐる認識と説明責任を持つ文化を構築するために役立ちます。AIとSaaSベースのスタートアップ企業についての詳細は、第7章で説明しています。

助言：CSAのAIワーキンググループは、AIの導入とそれに伴うリスクについて、以下の調査結果を発表しました。

シャドーアクセス：IAM Considerations for Zero Trust & AI | CSA AI Core Security Responsibilities | CSA

AIレジリエンス：Benchmarking AI Governance & Compliance | CSA

原則から実践へ：Responsible AI in a Dynamic Regulatory Environment

4.1.5 リスクレジスタ

リスクレジスタは、すべてのリスク管理活動のマスターリファレンスポイントです。確率、影響、脅威、脆弱性、影響を受ける資産、リスクレベルなど、すべてのセキュリティリスクに関する重要な情報が含まれています。

リスクレジスタにより、組織はリスク軽減の取り組みに優先順位を付け、監視することができます。リスクレジスタの管理と維持には様々な方法がありますが、国際標準化機構（ISO）やNISTなどの業界標準に沿ったモデルを採用することをお勧めします。

さらに、組織は、外部監査人がコンプライアンスイニシアチブの一環としてリスクレジスタを調査することが多いことに留意する必要があります。したがって、レジスタを管理し、最後に変更した日付を記録することが重要です。このようなレジスタの管理は、毎年更新されるスプレッドシートを使えば比較的簡単かもしれません。時間をかけて更新頻度を高め、会社のセキュリティ作業計画と統合して、リスクと緩和策を一致させる必要があります。ステークホルダーがプロセスに加わり、ビジネス環境が拡大するにつれ、プロセス全体を合理化するために、専用のリスクマネジメントシステムの導入を検討することが有益な場合があります。

4.1.6 リスク軽減／リスク管理プロセス

リスク管理には、リスクを特定、分析、評価し、許容可能なレベルに維持するためのプロセスが含まれます。これには、利害関係者と協力してさまざまなポリシーオプションを検討し、リスク評価やその他の関連要因を考慮し、適切な予防およびコントロール戦略を選択することが含まれます。これらのコントロールは、費用対効果と組織への影響のバランスを取る必要があります。
リスク管理プロセスには通常、以下のものが含まれます。

- **スコープの決定**：リスクマネジメントプログラムの境界線の設定。
- **関連資産の特定**：リスクのある情報資産を特定し、その侵害がもたらす潜在的な影響を評価するために、情報資産を目録化し、評価するプロセス。
- **リスクアセスメント**：関連する適用リスクを決定するプロセス。これには、脅威と脆弱性を特定し、影響と可能性を分析してリスクレベルを決定し、リスクが許容範囲内にあるかどうかを評価することが含まれます。
- **リスク対応**：特定されたリスクを管理するための適切な緩和策の選択。
- **コミュニケーション**：特定されたリスクに関連する情報を共有するプロセス。リスクコミュニケーションは通常、組織内の意思決定者や利害関係者の間で行われます。スコープ、評価されたリスク、およびアクションプランは、オープンなコミュニケーションとモニタリングを維持することにより、常に最新かつ適切な状態に保たれます。

社内の従業員にこれらのステップを実施する専門知識を持たないスタートアップ企業は、リスクアセスメントが最も一般的である場合、特定のプロセスを実行するために外部のコンサルタントに依頼するこ

とを選択することができます。これは今後、会社が頼りにしていける良い出発点になるかもしれません。

4.2 クラウドセキュリティにおけるプライバシーとデータ保護の考慮点

4.2.1 パーソナルデータの理解

パーソナルデータとは、「データ主体」として知られる、特定または識別可能な自然人に関連するあらゆる情報を指します。これには以下が含まれますが、これらに限定されるものではありません：

- **識別子**：氏名、住所、写真、識別番号、利用データ、およびオンライン識別子（IPアドレス、クッキー）
- **特定カテゴリー**：人種または民族的出身、政治的意見、宗教的または哲学的信条、労働組合への加入、遺伝子および生体情報、健康情報、および個人の性生活または性的指向に関するデータ
- **その他の「機微」情報**：特別なカテゴリー、未成年者、通信データ、社会保障番号、正確な地理的位置、金融口座番号とアクセスコード、および「侵入的（intrusive）」と認識されるあらゆる情報。

4.2.2 重要な考慮事項

1. **透明性とコミュニケーション**：
    a. データの処理と保護方法について、顧客との透明性を維持します。
    b. データ主体が権利を行使するための明確なコミュニケーション手段を提供します。
    c. ウェブサイトまたはプラットフォームに「プライバシー通知とポリシー」を掲載します（データコントローラである場合）。
2. **データの最小化と保持、目的の制限**：
    a. 業務に必要なデータのみを収集し、必要な期間だけ保持します。
    b. サービス提供、製品改善、マーケティング、セキュリティ、取扱い、法的義務など、データ利用の種類ごとに正確な理由を理解し、文書化します。
    c. クライアントが「所有」する情報、すなわちあなたの会社がデータプロセッサである場合、保存期間および保存目的を決定するのはクライアントであり、あなたの会社ではありません。
3. **データ主体の権利（Data Subject Rights（DSR））**：
    a. GDPRなどのデータ保護法に基づくデータ主体の権利の遵守の確保。これらの権利には、個人データへのアクセス、修正、消去、処理の制限、およびデータポータビリティが含まれます。
    b. これらの要請を処理するための明確な手順を確立します。情報が構造化された形式でない場合、要求が過剰である場合、またはデータがあなたの会社の事業運営に必要である

場合、データがあなたの会社によって「所有」されていない場合、管轄区域によっては一部の権利が適用されない場合があることに注意してください。

c. フェーズ1（インセプション）とフェーズ2（成熟段階）では、ほとんどの組織で、社内手続きを使用してデータ主体の要求に手作業で対応することができます。しかし、フェーズ3（成長）、または大量のリクエストがある場合は、データ削除と情報リクエスト処理の自動化プロセスを導入することをお勧めします。

4. **ベンダー管理とデューデリジェンス**：
   a. お客様のために個人データを保管または処理するすべての業者のリストを維持し、その業者のサービス内容および保有する情報の種類を記載します。
   b. フェーズ2およびフェーズ3：ベンダーおよびサービスプロバイダーとの契約に、データ保護条項または規制要件に沿ったデータ処理契約（DPA）を含めるようにします。
   c. フェーズ3：クラウドサービスプロバイダー（CSP）および個人データを保存または処理するその他のベンダーに対するデューデリジェンスを徹底し、堅牢なデータ保護対策が実施されていることを確認します。
5. **従業員/労働組合員**：
   a. アクセス制御を導入し、権限を定期的に見直して、権限を与えられた担当者のみがパーソナルデータにアクセスできるようにし、アクセスが自動的に記録されるようにします。
   b. 全従業員が機密保持誓約書の対象となるようにします。
   c. フェーズ2とフェーズ3：全従業員がプライバシーとセキュリティに関する定期的なトレーニングを受け、意識を高めます。
6. **データレジデンシーと主権**：
   a. CSPのデータセンターが、顧客の運用地域のデータレジデンシー要件に準拠していることを確認してください。一般的に、EUデータは適切な保護措置が講じられない限りEUに留まるべきで、これには例えば、(i)EU委員会の妥当性決定（すなわち、イスラエルが個人データに適切な保護を提供していると認められているため、イスラエルへの移転はOK）、(ii)標準契約条項（SCC）、(iii)拘束力のある企業規則（BCR）などが含まれます。
7. **インシデントレスポンスと侵害管理**：
   a. フェーズ1：基本計画：データ侵害を特定、報告、および対応するための明確なプロセスを定義します。これは、役割、責任、およびコミュニケーションチャネルを概説した簡単な文書でも構いません。
   b. フェーズ2と3：潜在的なデータ侵害に効果的に対処するためのインシデント対応計画を策定し、定期的に更新します。
8. **暗号化とデータ保護**：
   a. 暗号化は、GDPRやその他のデータ保護法への準拠を達成するために役立つ技術です。必須ではありませんが、許可された関係者しかアクセスできないように情報を読み取り不可能な形式に変換することで、データセキュリティを強化することができます。情報が暗号化されている場合、暗号化によって未認可な第三者にはデータがわからなくなるため、データ侵害を報告する必要性を防ぐこともできます。

9. **プライバシー・バイ・デザイン：**
    a. プライバシーを製品やサービスの開発に最初から統合し、課題が発生する前に予防すること、プライバシーをデフォルトで設定すること、プライバシーをシステム設計に組み込むこと、ライフサイクル全体を通じてデータを保護すること、透明性を確保すること：利害関係者にデータ処理を明確にすること、ユーザーを尊重すること：プライバシーのデフォルトやオプションを提供することなどの事前対策に重点を置きます。

4.2.3 データ保護責任者（DPO）を任命する場合、またはプライバシー専門家に相談する場合

複雑でリスクの高いデータ処理業務

フェーズ1（インセプション）とフェーズ2（成熟）：

- **役割：**DPOはデータ保護コンプライアンスを監督します。
- **外部 vs.内部**：外部採用、内部配属、パートタイム、またはフルタイムを問いません。組織内では、利益相反がない限り、DPOは他の職務を兼務することができます。特に、個人データの処理目的および処理手段を決定する場合はなおさらです。
- **資格**：データ保護法に関する専門知識、法律またはITのバックグラウンドがあることが望ましいです。特に資格は必要ありません。関連資格：Certified Information Privacy Professional (CIPP)
- **必要条件**：モニタリングや機密データを含む大規模なデータ処理を伴う中核的な活動でない限り、これらは必ずしも必要ではありません。しかし、DPOを任命することで、顧客、パートナー、および投資家との信頼を醸成することができます。

フェーズ3（成長段階）：

- **役割：**DPOはGDPRコンプライアンスを確保し、データ保護戦略を策定し、意識を高めます。
- **任命**：これは、データ処理の増加による成長段階には非常に重要です。
- **ターゲット**：法令遵守の徹底、個人データの保護、およびデータ保護の実践に関する従業員の教育。

4.2.4 主な規制の枠組みとコンプライアンス

注：プライバシー情報保護義務とその適用範囲は、企業の地理的な活動場所に大きく依存します。例えば、ブラジルで事業を行う場合、またはブラジルの個人からデータを収集する場合、ブラジルのLGPDの対象となる可能性があります。特筆すべきは、GDPRがデータ保護のほとんどの側面において世界的

な「ゴールドスタンダード」であり続け、世界中のプライバシー慣行と規制上の期待に影響を与えるベンチマークを設定していることです。

ここでは、適用される可能性のあるプライバシーおよびデータ保護に関する法律を紹介します。

- **General Data Protection Regulation (GDPR):**企業の所在地に関係なく、EU居住者の個人データを処理するすべての企業に適用されます。
- **California Consumer Privacy Act (CCPA):**年間総収入が2,500万ドルを超える場合、10万人以上のカリフォルニア州居住者または世帯の個人情報を購入、販売、または共有する場合。
- **Israel's Protection of Privacy Law and Regulations:**この法律は、あなたの会社がイスラエルにある場合に適用されます。「データベース」上の個人データセットの取り扱いに関する規則を定め、場合によっては、プライバシー情報保護局を通じたデータベース登録を義務付けています。
- **Health Insurance Portability and Accountability Act (HIPAA）**：米国で医療情報を取り扱う団体に適用され、医療データ保護の基準を定めています。

4.3 サードパーティリスク管理

4.3.1 識別

一般的なスタートアップ企業は、さまざまな目的のために複数の外部サービスプロバイダーに依存することがよくあります。この章では、主に2つのタイプのサードパーティに焦点を当てます：1つは、企業のデータやシステムにアクセスする人的サービスに関する、外部委託の従業員、アドバイザー、請負業者、ITプロバイダーなどです。共通しているのは、人間がアクセスを受け取るということです。

サードパーティのもう一つのタイプは、ソフトウェアプロバイダーです。平均的な企業では、何十、何百ものソフトウェアプロバイダーを日々の活動に利用しています。ソフトウェアプロバイダーの中には、IT部門や情報セキュリティ部門の目をかいくぐりやすい無料版を提供しているところもあることを考慮する必要があります。情報セキュリティを監督する者が早期に関与することは、意思決定を行う者がコストを優先しすぎることでセキュリティを不当に損なうことがないようにするために不可欠です。

サードパーティのリスクを管理する最初のステップは、社内で積極的に利用されているサードパーティを特定することです。出発点としては、現在の契約と支払いをすべて見直し、この情報を技術的なITツールでクロスチェックするのがよいでしょう。企業文化にもよりますが、部門マネージャーやチームリーダーに、使用しているソフトウェアについて尋ねてみるのもよいでしょう。
第二のステップは、新しいサードパーティ、請負業者、ソフトウェアベンダーを評価し、オンボーディングするための標準的なプロセスを確立することです。このプロセスは、一貫性とコンプライアンスを確保するために、全従業員に義務付けられるべきです。

インベントリには、現在および将来のすべてのサードパーティを文書化する必要があります。このインベントリには、プロバイダーの名前、提供するサービス、会社の所有者、関係するデータの機密性な

ど、必要不可欠な詳細を含める必要があります。このインベントリを常に最新の状態に保つためには、定期的な見直しが不可欠です。

4.3.2 最小限のセキュリティ要件（アクセスベース）

サードパーティと契約する際には、複数の考慮事項に対処する必要がありますが、それらはすべて、データの機密性とサービスの重要性から始まります。

新たな第三者契約の承認プロセスを明確に定めた方針を確立します。このポリシーは、IT、情報セキュリティ（InfoSec）、および法務の主要部門の関与を義務付け、包括的な監督とコンプライアンスを確保する必要があります。

情報セキュリティの観点からは、包括的なリスクアセスメントの実施が不可欠です。この評価には、サードパーティプロバイダーのデューデリジェンス、セキュリティ対策の評価、ISO27001やSOC2（Service Organization Controls）などの関連規格への準拠が含まれます。

会社のデータやシステムにアクセスできる外部の請負業者については、以下の要件を考慮してください。

- **秘密保持契約（NDA）**：これは最も一般的な担保条項です。契約書では、プロバイダーは機密情報や機微情報を保持することに同意します。
- **多要素認証（MFA）**：MFAなどの強力な認証を使ってシステムにログインします。
- **パーソナライズされたアクセスクレデンシャル:**外部契約者に提供されるアクセスはパーソナライズされ、資格情報が共有されないようにします。
- **マルウェア対策ソリューション**：請負業者がサービスを提供するために使用するすべてのエンドポイントに、信頼できるマルウェア対策ソフトウェアを要求します。
- **オペレーティングシステムの定期的な更新**：オペレーティングシステムの定期的な更新を維持します。
- **保存中データの暗号化**：エンドポイントに保存された企業データを暗号化し、不正アクセスや開示から保護します。さらに、データ漏洩のリスクを最小限に抑えるために、データのダウンロードをローカルマシンに制限することも検討すべきです。
- **セキュリティ侵害の即時報告**：請負業者に対し、セキュリティ侵害やインシデントが判明した場合は直ちに報告することを義務付けます。
- **ポータブルメディアの禁止**：USBドライブなどのポータブルメディアに会社のデータを保存することを禁止します。
- **監査**：この要件を追加すると、定義されたセキュリティ要件への準拠を検証するための監査を実施できるようになります。会社または会社の代理人がこれを行うことができます。

提供されるサービスの性質に応じて、必要に応じて追加要件を追加することができます。

可能な限りコントロールを徹底することが一般的には望ましいですが、必ずしも実現可能とは限りませ

ん。いずれにせよ、これらの要件はすべて請負業者との契約書に明記する必要があります。

4.3.3 リスクアセスメント

さまざまなサービスを提供するために外部機関を利用することは、通常、管理しなければならないリスクを生み出します。これは、組織のシステムに接続しているサードパーティや、機密データを扱っているサードパーティ、あるいは、業務運営に不可欠な機能を実行するサードパーティにとって非常に重要です。サードパーティと関係を持つ場合、そのセキュリティ慣行、関連規制への準拠、財務的安定性を評価するための徹底的なデューデリジェンスを実施することは、ほんの始まりに過ぎません。企業は、より広範なリスク管理プログラムの一環としてサードパーティリスクを管理する必要があります。

4.3.3.1 ベンダー監査

特定の機能のアウトソーシングやサービスプロバイダーの利用を検討する場合は、契約期間中、ベンダーの管理体制の適切性を監査し、監視する必要があります。これによって、コストの圧迫やベンダーの業務優先順位の変化によって、セキュリティ対策が時間の経過とともに疎かになることがなくなります。組織はこれを達成するために、適切なコントロールが効果的に機能していることを確認するための第三者機関による監査やサードパーティ施設への訪問など、いくつかの戦略を採用することができます。

外部監査人による独立監査は、ベンダーのコントロール、プロセス、および関連基準や規制への準拠について客観的な評価を提供します。これらの監査には、ベンダーのセキュリティポリシー、データ保護対策、インシデント対応計画、ISO 27001などのフレームワークへの準拠のレビューが含まれます。このような監査を定期的に実施し、ベンダーのコントロールとコンプライアンスを監視することが不可欠です。

4.3.3.2 アンケート

サードパーティベンダーのセキュリティ成熟度を測る一般的なツールは、セキュリティアンケートです。サードパーティのセキュリティコントロールを評価するのに役立つ、さまざまなセキュリティ領域の質問が含まれています。企業は、独自のセキュリティ懸念に合わせた質問を作成することもできますし、CSA Consensus Assessment Initiative Questionnaire（CAIQ）のようなオンラインで標準化された質問票を利用することもできます。コントロールがどのように実施されているかを理解するためには、特定の質問に対して説明や証拠を求めることが不可欠です。

中小企業では、このようなセキュリティアンケートの配布や評価は、手作業で行われることが多いです。しかし、スケーラビリティと効率性の必要性が高まるにつれ、自動化されたソリューションの探求が不可欠になります。自動化ツールとベンダリスクマネジメントプラットフォームは、プロセスを合理

化し、評価の一貫性を確保し、長期にわたってベンダーのセキュリティリスクを効果的に管理できます。

助言：CSA Security, Trust & Assurance Registry（STAR）プログラムは、クラウドプロバイダーのためのセキュリティアシュアランスプログラムです。STARを利用することで、SaaSベースのスタートアップ企業はクラウド保証プロセスにおけるアンケートや顧客との摩擦を減らすことができます。
STAR | CSA

4.3.4 ベンダーレジストリ

ソフトウェアプロバイダー、アドバイザー、請負業者など、ベンダーの包括的なリストを維持することは、いくつかの理由から重要です。

第一に、すべての外部契約とそのサービスの明確な概要を提供することにより、組織内の透明性と説明責任を確保します。

第二に、このようなリストは、特にデータ保護とサイバーセキュリティにとって重要な分野におけるベンダーのセキュリティとコンプライアンスの状況を評価し、監視を可能にすることで、リスク管理を容易にします。サードパーティのサービスから発生する可能性のある脆弱性を特定するのに役立ちます。さらに、セキュリティ侵害やコンプライアンス監査が発生した場合、すべてのベンダーとの契約に関する詳細な記録があれば、潜在的な侵害原因の特定や規制機関へのデューデリジェンスの実証が容易になります。

最後に、このプラクティスは、外部サービスに関連するコストに関する洞察を提供することにより、戦略的プランニングと予算編成を支援し、効率化が可能な分野や投資が必要な分野を特定するために役立ちます。

通常、財務チームは、IT部門、法務部門、および情報セキュリティ部門と連携して、すべてのサードパーティの契約文書を管理します。このリポジトリには、提供されるサービスに関連する事業部門、第三者がアクセスできるデータの分類または機密性、契約が有効であるかどうか、およびその他の関連情報を含める必要があります。この文書の定期的な更新と見直しは、コンプライアンスを継続し、ベンダーのサービスや関連リスクの変更に対応するために極めて重要です。

4.3.5 ベンダーの解約

企業はベンダーサービスを無期限に利用しないのが一般的です。契約が締結された場合、シームレスな移行を確実にし、会社の利益を保護するために、いくつかの側面を慎重に管理する必要があります。これには**ナレッジトランスファー**や**データマイグレーション**が含まれ、ベンダーが保有するデータやナレ

ッジを企業や別の指定ベンダーに確実に戻すことができます。例えば、クラウドサービスプロバイダーが変更される場合、損失やダウンタイムなしに新しいプロバイダーにデータを移行することが極めて重要です。

データの削除：解約するベンダーが所有する企業データが、セキュアに削除されることを確認します。これには、データ破壊の証明書や証拠を取得することも含まれます。削除処理にバックアップコピーが含まれていることを確認してください。

サポート：移行中に発生した課題に対処するため、ベンダーが終了後もサポートを提供できることを確認します。これには、移行されたシステムのテクニカルサポートや、提供されるサービスに関する問い合わせのサポートなどが含まれます。

ベンダーの終了処理は、確立された変更管理プロセスの一環として行われるべきであり、すべての関連する利害関係者が終了手順に関与していることを確認する必要があります。これには、IT部門、研究開発部門、財務部門、およびベンダーのサービスによって直接影響を受ける業務部門が含まれます。これらの利害関係者が関与することで、すべての契約上の義務が果たされ、リスクが評価され、軽減され、会社が関連する法律や規制を遵守することが保証されます。

助言：IaaS/PaaSでは、スタートアップ企業はクリプトシュレッダーと呼ばれるテクニックを使用することで、データ消去の保証を向上させることができます。ほとんどのSaaS CSPには顧客管理鍵のオプションがないため、この手順を SaaS プラットフォームに実装するのは困難です。

44 コンプライアンス

スタートアップ企業は、サイバーセキュリティ要件の実施に加え、投資家、ビジネスパートナー、顧客、および規制当局に対してサイバーセキュリティポスチャーを実証する必要があります。このデモンストレーションはしばしばコンプライアンスと呼ばれます。

コンプライアンス（サイバーセキュリティポスチャー）を証明するために、複数の方法を使用することができます。これらの方法には次のようなものがあります。

- セキュリティアンケートへの回答
- 要件遵守の証拠の提供
- ペネトレーションテストの報告書の提出
- スタートアップ企業の初期段階を経た後に、世界的に認知されたフレームワークからの外部監査報告書または認証の取得

多くの企業がベンダーの選定や承認プロセスにおいてコンプライアンスを要求しているため、コンプライアンスもビジネスを活性化します。

スタートアップ企業のライフサイクルの最初の段階（インセプション）では、コンプライアンスを文書化し、顧客やその他の利害関係者に提示できるようにすることが推奨されます。規制の厳しい領域（金融サービス、医療、重要インフラストラクチャなど）のスタートアップ企業は、市場参入を可能にするために必要となるコンプライアンス要件をロードマップに追加する必要があります。

フェーズ2（成熟期）では、スタートアップ企業は、本章で後述する一般的なサイバーセキュリティコンプライアンスフレームワーク（SOC2 または ISO27001）の少なくとも1つと、市場参入戦略をサポートするドメイン／セクター／地理的フレームワークを導入する必要があります。このフェーズでは、スタートアップ企業は通常、外部のコンサルタント（CISO as a ServiceまたはGRCの専門家）を利用してコンプライアンス業務を支援します。

フェーズ3（成長段階）では、マーケティングウェブサイト（別名「トラストページ」）での証拠収集、コンプライアンス活動、セキュリティポスチャの報告を自動化するコンプライアンスプラットフォームの導入を推奨します。さらに、コンプライアンスプラットフォームは、最小限の追加オーバーヘッドで複数のフレームワークをサポートします。

また、ビジネスの成長をサポートするコンプライアンスフレームワークのリストを積極的に確立し、新しいフレームワークや変更されたフレームワークを追跡し、サイバーセキュリティのロードマップの一部としてそれらのサポートを計画することが推奨されます。

助言：SaaSベースのスタートアップ企業は、顧客のサードパーティリスク管理プログラムの一環として、多くの場合、複数の顧客アンケートに回答する必要があります。CSA Security, Trust & Assurance Registry（STAR）プログラムは、クラウドプロバイダーのためのセキュリティ保証プログラムです。STARを利用することで、SaaSベースの新興企業はクラウド保証プロセスにおけるアンケートや顧客との摩擦を減らすことができます。
STAR | CSA

4.4.1 セキュリティフレームワーク

情報セキュリティのための最も一般的な2つのコンプライアンスフレームワークは、SOC2とISO27001です。ほとんどのB2B SaaSベースのスタートアップ企業は、顧客の要求によってこれらのフレームワークを採用し、その初期段階（通常はフェーズ2の初期段階）でそれらを達成します。コンプライアンスは独立した監査によって証明されます。

SOC2：
スタートアップ企業は、セキュリティ、可用性、処理の完全性、機密性、またはプライバシーコントロールが効果的に運用されていることをビジネスパートナーや顧客に対して保証し「信頼構築」するために、公認会計士による**SOC2監査**に備える必要があります。このプロセスにおいて、監査人は、完全に運用され有効なコントロールの証拠を求めます。スタートアップ企業は、準備プロセスを独自に実行することも、サードパーティのコンサルタントを使用して実行することもできます。

ISO27001：
ISO27001もかなり一般的です（EUベースの顧客にとっては、より一般的です）。これは、情報セキュリティマネジメントシステム（ISMS）と管理策のリスト（good practice controls - 附属書 A）の実施に基づいています。認定された認証機関の外部審査員が審査を行い、例えば顧客やウェブサイトに提示する認証書を提供します。**ISO27001認証**は、毎年行われるサーベイランスバリデーション審査（1年目は本審査、2年目と3年目はサーベイランスバリデーション、4年目は本審査、といった具合）に基づいて3年間有効です。

4.4.2 データ保護規制

SOC2 や ISO27001 などのセキュリティに関する基本的なコンプライアンスに加え、個人を特定できる情報 (PII) などの特定の種類の情報を処理するスタートアップ企業は、データ保護に関する法律や規制を遵守する必要があります。顧客の地理的な位置とデータ収集のタイプに応じて、遵守すべき事項が異なります。データの最初の項目の収集の時点から遵守を始める必要があります。こうしてスタートアップ企業は、設立初期段階からデータ保護規則に対処できます。

データ保護コンプライアンスフレームワークの例：

- PCI-DSS（Payment Card Industry-Data Security Standard）：ペイメントカード情報（PCI）を収集する予定の場合。
- HIPAA：Protected Health Information（PHI）を収集する予定の場合。
- プライバシー規制（GDPR、CCPA）：個人を特定できる情報（PII）の収集を計画している場合は、第4.2章「クラウドセキュリティにおけるプライバシーとデータ保護の考慮事項」を参照してください。

4.4.3 業界ベースのフレームワーク

前述のコンプライアンスの枠組みや規制に加えて、スタートアップ企業の中には、顧客の市場分野や地理的な場所に基づいて、さまざまなサイバーセキュリティ認証の遵守を求められるところもあります。

- FedRAMP (US)：連邦政府機関にクラウドサービスを提供する企業向け。
- NIS2 (EU)：EU域内で重要インフラストラクチャーサービスを提供する企業向け。
- Cyber Essentials (UK)：英国でビジネスサービスを提供する企業向け。

4.4.4 より進んだ認証

一部のスタートアップ企業は、顧客への保証の提供やビジネス上の優位性の獲得を目的として、より高度なクラウドに特化した認証を取得しています。いくつか例を挙げます。

- ISO27018：パブリッククラウドコンピューティング環境における個人情報保護のためのクラウドプロバイダーのためのガイドラインを提供します。
- ISO/IEC 27017：クラウドサービスプロバイダーと利用者に特化した情報セキュリティのガイドラインとコントロールを提供します。
- CSA STAR Level 2：CSA STAR プログラムは、CSP（訳注：原文はCPSとなっているがCSPの間違いと思われる） のセキュリティ対策を保証します。

4.5 章のサマリー

	フェーズ1	フェーズ2	フェーズ3
リスクマネジメント	資産リストを作成して更新し、サプライチェーンパートナーを賢く選びましょう。	定期的に更新されるリスク登録簿の構築。BIAおよび緩和プロセスの実施。	影響分析、尤度、およびリスク対応を含む成熟した企業リスク管理計画
プライバシー	プライバシー・バイ・デザインの基礎を確立します。ターゲット市場に基づく関連規制のマッピング。	DPO（非常勤、通常は社外）を任命。最も関連性の高い規則を遵守します。	DPOの地位と責任を強化します。ビジネスニーズに基づき、遵守すべき規制を追加します。
サードパーティ	ベンダーの基本的な検証、NDA、最小限のセキュリティ評価。ベンダー管理はアドホックで、正式なプロセスがありません。	セキュリティアンケート、リスクアセスメント、およびベンダー登録が維持されています。	継続的なモニタリングと定期的な監査による包括的なベンダー管理プログラム
コンプライアンス	セキュリティに関する考慮事項を文書化し、セキュリティコントロールを実装します。	CISO（非常勤、通常は社外）を任命するか、GRCコンサルタントを雇います。SOC2またはISO27001の認証取得。	コンプライアンスプラットフォームとトラストページを展開し、ビジネス要件に応じて複数のフレームワークをサポートします。

5. ITセキュリティ

今日、ほとんどのスタートアップ企業は、社内のインフラストラクチャを最小限に抑え、コストを削減するためにクラウドサービスを活用し、最小限の体制でスタートしています。初期のITニーズは基本的なオフィスのインターネットアクセスに限られるかもしれませんが、成長する企業では責任も大きくなります。ITチームは、アイデンティティシステム、従業員のワークステーション、コラボレーションツール（電子メール、ビデオ会議、ファイル共有）などの重要なコンポーネントをセキュアにし、管理する必要があります。これらのサービスは組織のデジタル基盤を形成するため、クラウドソリューションが提供する俊敏性を維持しながらも、最初から堅牢なセキュリティ対策を導入することが不可欠です。

5.1 IT構造

5.1.1 フェーズ1

5.1.1.1

この段階では、スタートアップ企業は小さなグループです。オフボーディングとオンボーディングは手作業で行われ、BYOD（Bring-Your-Own-Device）が普及しています。親密なチーム環境であるため、セキュリティの緊急性は低く感じられるかもしれませんが、このフェーズで基本的なセキュリティコントロールを実施することが重要です：多要素認証（MFA）は、クレデンシャルの盗難から保護し、企業アカウントは、従業員が退職したときにビジネスの継続性を確保し、専用の管理者アカウントは、誤ったシステム全体の変更を防止します。これらの基本的な対策は、今すぐ実行するのが簡単で、企業の成長とともに不可欠なセキュリティの習慣を確立することができます。

助言：SaaSベースのスタートアップ企業の多くは、少なくとも初期段階では、ITの責任を最高情報セキュリティ責任者（CISO）の下に置いています。

5.1.2 フェーズ2

5.1.2.1

この段階では、ほとんどのスタートアップ企業が外部のITサービスを利用しています。外部ベンダーを自社のやり方に「慣れさせ」、スタートアップ企業におけるセキュリティの重要性を理解してもらうことが重要です。

5.1.2.2

ほとんどのスタートアップ企業はこの段階で集中管理ツールを導入し、ワークステーションのセキュリティと外部ベンダーのセキュリティポリシーの遵守の両方を監視できるようにします。理想的には、モバイルデバイス管理（MDM）ソリューションの使用を開始する時期です。

助言：MDMによるAppleデバイスの管理は、適切に設定しないと複雑になる可能性があるため、Macデバイスをグローバルに使用する場合は、管理ツールの機能に特に注意してください。

5.1.2.3

ほとんどの場合、ITドメイン内のさまざまなサービスに対する管理者アクセス権を外部プロバイダーに提供する必要があります。専用ワークステーション、VM、またはその他のソリューションを提供することで、ITベンダーをハッキングしても、ハッカーが簡単にネットワークに接続できないようにすることを検討してください。ここで重要なのは、最も弱いリンクという概念です。管理業務に使用されるすべてのワークステーションは、その所有者や操作者に関係なく、同じセキュリティ基準に設定されるべきです。

5.1.3 フェーズ3

5.1.3.1

企業が複数の拠点に成長し、IT管理が複雑化すると、ITの内部SLAが課題になります。

5.1.3.2

退職する従業員のバックアップとデータへのアクセス、ITハードウェアの管理、モニタリング、自動オンボーディング、およびオフボーディング。 ITサービスはサードパーティのリスク管理などのガバナンス方法論に従っており、BCP/DR プロセスは ITサービスに対して完了しています。

5.2 コラボレーションサービス

ほとんどのスタートアップ企業は、ドメイン名を取得し、Microsoft 365やGoogle Workspaceなどのコラボレーションサービスを導入することからITの旅を始めます。これらのサービスには、eメール、チャット、ドキュメント共有、eミーティングサービス、IDP（アイデンティティプロバイダー）などがあります。後の段階でコラボレーションサービスが追加されるかもしれませんが、これらのサービスはスタートアップ企業のセキュリティポスチャにおいて重要な基盤であり続けます。長期的には、コラボレー

ションサービスもスタートアップ企業の成熟に合わせて進化させる必要があります。これには、これらのサービスに追加のツール、コントロール、および検出応答技術を統合することが含まれます。次のセクションでは、一般的な成熟のステップのリストを示します。

5.2.1 認証

5.2.1.1

シンプルなパスワードポリシーを作成します。長いものであるほどよく、他は重要ではありません。少なくとも10文字以上とし、パスフレーズの選び方を全員に指導します（例えば、「長いほど良い」または「シンプルなほどよい」など）。

5.2.1.2

利用するすべてのサポート対象サービスにおいて、二要素認証（2FA） を必須として有効にします。たとえ自動で強制できなくても（たとえば、手動で設定するとしても）、すべての管理者アカウントに2FAを強制します。管理者には物理的な認証デバイスを推奨します。

5.2.1.3

個人アカウントではなく、企業アカウント（例：Googleでログイン、Microsoftでログイン）でログインするように、全員に指示します。

5.2.1.4

モバイルアプリベースのMFAは、一般的にテキストメッセージに基づく認証よりもセキュアです。SMS認証は、なりすましやフィッシング（スミッシング）に対して脆弱です。

5.2.1.5

個人のソーシャルメディアアカウントに2FAを追加することを教え、推進します。マーケティング／営業チームは個人アカウントを使用するため、企業リスクとなります。

5.2.2 クラウドアプリにおける役割と権限

5.2.2.1

新しい社内横断アプリ（マーケティング、営業、一般的な用途、その他の目的）を導入しますか？最初にすべきことは、管理者の役割とユーザーの役割を調査することです。それぞれの能力を理解し、ユーザーの役割ポリシーを定義します。（誰が何を取得するか、など）

5.2.2.2

一般的に、ユーザーはユーザーロールを取得する必要があります。

5.2.2.3

サードパーティプロバイダーに注意してください。彼らは、何をしなければならないかに関係なく、管理者ロールを要求する傾向があります。たとえば、マーケティングチームが SEO 代理店を雇って、Hubspot (マーケティングツール) を使用して広告キャンペーンを管理するとします。 この場合、キャンペーンマネージャーロールを作成できますが、一部の代理店は、制限がなく、チームにユーザーを追加したり、営業チームが使用するプロパティを変更したり、ロックすることなどができるスーパー管理者ロールを要求する場合があります。

- **フェーズ1**：創業者のCTOがすべてを行います。
- **フェーズ2**：アプリごとに、アプリのセキュリティに関してCISO/CTOの監督の下で働く関連チームの管理者を指定することができます。
- **フェーズ3**：これらすべてのアプリを管理および監視するために、サードパーティのリスク管理プロセスを導入する必要があります。

5.2.3 権限の共有

5.2.3.1

権限の共有は、クラウドオフィススイートで作業する上で最も重要な側面の1つです。従業員は、URLをコピーして共有したり、共有ボタンを使ってドキュメントを共有したりしがちです。共有権限は最初からコントロールすべきです。後から追加することはできません。なぜなら、それが習慣となり、習慣はなかなか変えられないからです。

- **フェーズ1**：外部共有を防止し、すべての関連リソースに適用されるようにします。
- **以後のフェーズ**：成熟に伴い、PIIの検出、情報の分類（eDiscovery）、アクセスの管理（DSPM/IRM）、データ漏えいの検出（DLP）の機能を追加します。

5.2.3.2

社員が退職する際に、データや共有情報が失われないような手順を作成します。クラウドドライブの構造によっては、このような障害が発生することがあります。

5.2.4 高度なツール

5.2.4.1

ほとんどのコラボレーションサービスには、追加のセキュリティ機能（拡張モニタリング、IRMと暗号化、DLP、 vault ）を備えたサブスクリプションオプションがあります。サービスが成熟するにつれ、要件に応じてライセンスを拡張し、機能を追加します。コラボレーションサービスにはスタートアップIdPが含まれることが多いため、拡張モニタリングは優先事項の1つです。

5.3 ワークステーションセキュリティ

5.3.1 セキュリティアップデート

5.3.1.1

セキュリティアップデートは、セキュリティ戦略の重要な要素です。すべてのデバイスが一貫してアップデートされていることを確認することは、脆弱性と脅威から保護するために不可欠です。セキュリティ更新を管理するアプローチは、スタートアップ企業の進化する能力とリソースを反映して、3つの成熟度レベルに分けることができます。

- **フェーズ1**：この初期段階では、スタートアップ企業には包括的なセキュリティ更新やパッチ管理計画を策定する時間やリソースがないかもしれません。更新は、可能な限りアドホックに行われます。チームメンバーには、定期的にアップデートを手動で確認し、適用するよう促します。特にオペレーティングシステムや、ウェブブラウザ、コミュニケーションツールなどの重要なソフトウェアについては、重要なセキュリティアップデートの優先順位を決めます。
- **フェーズ2**：スタートアップ企業が成長し、リソースが確保できるようになったら、セキュリティ更新を管理するための基本的なプロセスを確立します。アップデートを適用する方法とタイミングを定義する明確なアップデートポリシーを策定します。アップデートのモニタリングと適用の責任を特定の個人またはチームに割り当てます。すべてのデバイスが自動的にアップデートをダウンロードするように設定されていることを確実にします。ただし、インストールにはユーザーの介入が必要になる場合があります。さらに、リスク管理アプローチを導入し、新しいパッチによる潜在的な課題を軽減するために、最新リリースから1つ遅れたアップデートを選択することもできます。

- **フェーズ3**：この成熟した段階で、すべてのデバイスにアップデートポリシーをデプロイし、実施するための集中型ツールを実装します。すべてのデバイスが、ユーザーによる上書きを許可せずに、自動セキュリティ更新プログラムをダウンロードしてインストールするように設定します。スタートアップ企業のリスク選好やシステムの可用性の重要性に応じて、予防措置として最新リリースから1つ遅れてアップデートを行う戦略を維持することを検討してください。この方法を選択する場合は、デプロイメント前に徹底的なテストを行うようにしてください。更新プロセスを定期的に監査および見直し、コンプライアンスを確保し、課題があれば速やかに対処します。

5.3.2 ユーザーの役割と権限

5.3.2.1 Windows:

初期から非管理者ユーザーポリシーを実装します。企業内のほとんどのロールでは管理者権限を必要としません。ローカル管理者権限を必要とするアプリケーションはまれで、通常は時代遅れなものです。現代的な選択肢を探しましょう。

5.3.2.2 Mac:

管理者以外のユーザーポリシーを導入することは、デバイス管理ツールなしでは難しいかもしれませんが、セキュリティを維持するためには不可欠です。

5.3.3 エンドポイントセキュリティ対策

5.3.2.1 フェーズ1：

Windows：Windows Proバージョンに含まれているWindows Defender無料版を導入します。Windows Proバージョンに内蔵されているBitLockerでノートパソコンを暗号化します。組織でOffice 365（O365）を使用している場合は、組織のO365アカウントに暗号化鍵をバックアップします。そうでない場合は、アクセス制限のある共有フォルダに保存してください。
Mac：ファイアウォールと暗号化（FileVault）を有効にし、暗号化鍵を集中管理された場所にバックアップします。

5.3.2.2 フェーズ2：

専用の管理リソースが限られている可能性があるため、自動化、デプロイメントの容易さ、およびパフォーマンスを優先順序付けして、クロスOSの集中型エンドポイントセキュリティソリューションを導入します。すべてのノートパソコンに選択したソリューションが装備されていることを確認します。

5.3.2.3 フェーズ3：

セキュリティ強化のため、MDR（Managed Detection and Response）サービスの導入を検討します。

5.3.4　デバイスコントロールと集中管理

5.3.4.1フェーズ1：

Windows:
O365（Active Directoryの有無に関わらず）を使用している場合は、O365製品ライセンスを持たないコンピュータであっても、O365ユーザーを作成して、すべてのコンピュータをO365ドメインに追加します。これにより、ドメインコントロールが一元化されます。O365を使用していない場合は、最初から中央管理の導入を検討してください。

Mac:
Apple Business ManagerにMacを登録することで、ユーザーによるデバイスロックの可能性を回避できます。すべてのリモート管理ツールは、デバイスを完全に所有するためにApple Business Managerを必要とするため、これはリモートワークにとって非常に重要です。費用はかかりますが、集中管理を強くお勧めします。

5.3.4.2 フェーズ2：

- 集中管理ツールの導入。オプションは以下の通りです：
    - ITプロバイダーが提供するITツールは、セキュリティに特化していないかもしれませんが、セキュリティポリシーをデプロイできます。
    - セキュリティ管理ツール（Jumpcloud、Intuneなど）
- それぞれに長所と短所がありますが、ツールがあるに越したことはありません。

5.3.4.3 フェーズ3：

すべてのプラットフォームでデバイス管理を統合する統合エンドポイント管理（UEM）ソリューションを導入します。セキュリティポリシー、アップデート、および構成のデプロイメントを自動化します。
業界の規制や基準へのコンプライアンスを管理するツールを導入します。一元化されたレポートダッシュボードを活用して、すべてのエンドポイントのセキュリティポスチャをリアルタイムで可視化します。
従業員向けに定期的なセキュリティトレーニングを実施し、デバイス管理とセキュリティ課題を管理する専任のサポートチームを設置します。

5.3.5 設定ツール

5.3.5.1 フェーズ1：

設定作業は手動で行います。

5.3.5.2 フェーズ2：

手作業による設定が負担になる場合は、外部のIT部門に一元化された設定ツールをデプロイしてもらうことを検討します。デプロイメント前に、ツールのITセキュリティと顧客分離機能を評価します。

5.3.5.3 フェーズ3：

社内のITチームにより、すべての設定が一元的に管理されるようにします。

5.4 リモートアクセス

リモートアクセスは、ITセキュリティ戦略において最も重要な要素の1つです。これは、潜在的にセキュアでないインフラストラクチャから企業のリソースにアクセスするためのセキュアな環境を提供することです。主な課題は、従業員が社内ネットワークに接続するために使用するデバイスをコントロール・可視化できないことです。パスワード、二要素認証（2FA）、物理的なハードウェアトークンなどの堅牢な認証方法を使用しても、従業員が外出先で友人のノートパソコンからログインするなど、これらの認証デバイスがセキュアでないデバイスから使用される場合のリスクは依然として存在します。これに対処するため、以下の成熟度レベルを通じてリモートアクセスソリューションを検討します。

このセクションは、第2章リモートアクセスのセクションの補足です。第2章では、IaaS/PaaS ワークロードへの運用および管理者アクセスについて言及していますが、本節では、 より一般的なアクセスタイプ（SaaS アプリケーションへのアクセスなど）に焦点を当てます。

5.4.1 フェーズ1：

この段階では、チームはおそらくIaaS/PaaS環境用のVPNと、様々なSaaSアプリケーション（GitHub、Jira、O365）への直接アクセスを持っているでしょう。強固で一意のパスワードなどの基本的なセキュリティ対策を実施し、すべてのアカウントで二要素認証（2FA）を有効にします。個人所有のノートパソコンを業務に使用することを奨励し、最新のセキュリティパッチを定期的にアップデートします。会社のリソースにアクセスするために、公共のデバイスや保護されていないデバイスを使用しないことの重要性を従業員に教育します。

5.4.2 フェーズ2

VPNに加えて、エンドポイントセキュリティソフトウェアを導入し、アクセスを許可する前にデバイスのセキュリティステータスを確認する必要があります。接続デバイスのセキュリティステータスに基づいてアクセスを制限する条件付きアクセスポリシーを実装します。

5.4.3 フェーズ3

Secure Access Service Edge（SASE）/ゼロトラストアーキテクチャ（ZTA）を採用し、すべてのアクセス試行を継続的に監視して検証します。生体認証や適応型多要素認証（AMFA）などの高度な認証方法を使用します。包括的なEDR（Endpoint Detection and Response）ソリューションを導入して、脅威をリアルタイムで検出し、対応します。定期的にリモートアクセスポリシーを監査および更新し、新たなセキュリティ課題に対応します。

5.5 オフィスネットワーク

SaaSアプリケーションの台頭、ダイナミックな料金プラン、中核となる事業活動に集中する必要性により、現代のスタートアップ企業はクラウドベースのソリューションを活用するようになりました。ローカルのオンプレミスネットワークはあまり普及しなくなり、ほとんどのスタートアップ企業はクラウドインフラストラクチャーを使ってすべてのワークロードを管理しています。

ITに関する検討事項とは別に、スタートアップ企業の創設者は、事業拠点をどこにするかという問題に必ず直面します。一般的なオプションは以下の通りです。

完全リモート：物理的なオフィススペース無しで営業します。
マネージドオフィスモデル（WeWorkなど）：時間単位のオフィスから、ITとネットワークインフラストラクチャーを管理する完全な専用エリアまで、幅広いオプションが用意されています。
自主管理オフィス：従来のリース契約で、スタートアップ企業自身がオフィススペースを管理します。

マネージドオフィスモデルは、多くの場合、小規模なスタートアップ企業に最適ですが、大企業にも適しています。企業が拡大するにつれて、ニーズに応じてリモートオフィス、マネージドオフィス、およびセルフマネージドオフィスの各拠点を活用するハイブリッドアプローチを採用する場合もあります。

専用のデータセンターを運営するには、物理的なスペース、専任の人員、冷却や電力管理などのユーティリティが必要になるため、スタートアップ企業には不向きです。その代わりに、IT機器をサードパー

ティのデータセンターにコロケーションしたり、クラウドIaaSプロバイダーを排他的に活用したり、ハイブリッドアプローチを採用したりといった選択肢が現実的です。

企業が完全なリモート化を選択せず、リース契約がITサービスをカバーしない場合、ルーター、スイッチ、アクセスポイント、プリンター、およびIoTデバイス（警報システムやデジタルカードリーダーなど）といった必要不可欠な機器をプロビジョニングする必要があります。これらは社内で管理することも、サードパーティのサービスプロバイダーにアウトソーシングすることも可能で、必要に応じてリモートワークロードに接続することができます。

5.6 企業ウェブサイト

このトピックでは、製品が別のプラットフォームで動作することを考慮し、企業のウェブサイトのマーケティング面に焦点を当てます。マーケティングサイトは、アプリケーションが一般に利用可能になる前から関連性があります。

マーケティングウェブサイトは、主に初期段階のスタートアップ企業向けに静的コンテンツを提供しているため、ホスティングの選択肢は無限にあります。

ここでは、最も一般的なウェブサイトのホスティングオプションと、どのユースケースに最も適しているかを説明します。

1. **IaaS上にデプロイされるセルフマネージドウェブサイト**：企業がウェブサイトのコンテンツを持っていれば、それをストレージバケットにアップロードするだけで、最小限の設定でサイトを立ち上げ、運用することができます。

   このモデルは、最小限の技術的な操作にこだわらない、静的なページのみのごく初期のスタートアップ企業に適しています。それはウェブサイトを管理する最も安い方法でしょう。

2. **完全アウトソーシング型ウェブサイト**：このモデルでは、あなたはほとんど何も気にする必要はありません。ウェブサイトは通常、ウェブサイトデザイナーによって提供され、デザイナーはコンテンツとホスティングの両方を担当します。その会社はドメイン登録とDNSを担当しています。

   このモデルは、ホスティングサービスを管理するオーバーヘッドを望まない、主に初期段階のスタートアップ企業に適しています。

3. **セルフマネージドオールインワンプラットフォーム**：コンテンツのホスティング、DNSレコードの管理、ドメインの登録、これらすべてを同じプラットフォームで実現します。CDNやWAFなど、その他の高度な機能を通常は利用可能です。

このモデルは、主に半成熟または成熟したサイトを持つスタートアップ企業に適しており、かなりの数の訪問者があり、前述の側面を自己管理する能力があります。

4. **セルフマネージド専用ホスティングプラットフォーム**：このモデルでは、ウェブサイトホスティングのためだけに専用サービスプロバイダーを使用します。このようなプロバイダーは通常、プレミアム機能と性能をサポートしています。

   このモデルは主に、多くの訪問者と大きな帯域幅を必要とする成熟したウェブサイトに適しています。それはおそらく最も高価なオプションになるでしょう。

5.7 章のサマリー

	フェーズ1	フェーズ2	フェーズ3
ITストラクチャ	セキュリティの本質的なプロセスである、ポリシーの導入と徹底から始めます。	ITパートナーを賢く選択し、中央IT管理ツールをデプロイします。	明確なSLAを備えた成熟した独立したITサービス。オンボーディング手続きおよびその他のITガバナンスプロセスの自動処理
コラボレーションサービス	基本的なセキュリティ：MFA、企業アカウント、管理者の分離	きめ細かな役割、任命されたSaaS管理者、および共有されたポリシー。IRMと暗号化の検討	モニタリングや検出、DLPなどの高度なツールの追加
ワークステーションセキュリティ	重要なコンポーネントの手動更新。基本的なセキュリティハイジーンに責任を持つようユーザーに奨励	すべてのWSの構成のベースラインを設定し、文書化されたポリシーによって強制します。OSのハードニングとアップデート機能に依存	中央管理ソリューションを導入し、ポリシーを実装します。リスクを更新するために、最新のポリシーとアドレスを構築
リモートアクセス	CSPのVPNサービスを利用します。SaaSに直接接続	ワークステーションのエンドポイントセキュリティ、条件付きアクセスなど、さらなるレイヤーの追加	異なる支店やSaaSアプリケーションにアクセスするための完全なSASE/ZT。すべてのワークステーションにEDR

6. セキュリティモニタリングとインシデント対応

6.1 イントロダクションとモチベーション

セキュリティモニタリングは、第一に組織が危険にさらされているかどうかを把握するために使用されます。組織が対応能力を欠いていたとしても、サイバー侵害に対する認識は不可欠です。すべては、モニタリングやロギングの手法を使って検知する能力から始まります。セキュリティモニタリングは、進化する脅威とトレンドを継続的に監視し、弱点（脆弱性）を特定し、組織内のアクティブな侵入と未認可な行動を検出することで、組織全体のセキュリティに対する状況認識を向上させ、インシデント対応プロセスをサポートする質の高いリスクベースの意思決定を可能にします。

侵害が検出されると、インシデント対応チームに連絡し、対応や顧客とのコミュニケーションを行うことができます。歴史が教えてくれるのは、顧客は、通知を受け、必要な緩和措置が取られる限り、企業の侵害行為を容認するということです。

IBMのレポートによると、平均時間と応答時間の統計値は以下になります。

- 全世界で、データ侵害を特定するために平均204日かかっています。
- 脅威インテリジェンスを使用している組織は、脅威を平均28日早く特定できます。
- 侵害の封じ込めに要した時間は平均73日です。
- 盗まれた、または漏洩したクレデンシャルを使用した侵害は、解決に最も時間がかかり88日でした（データ侵害のライフサイクルは328日）。
- ライフサイクルが200日未満のデータ侵害のコストは、200日以上のものより平均102万ドル低くなります。

6.2 方法論とテクノロジー

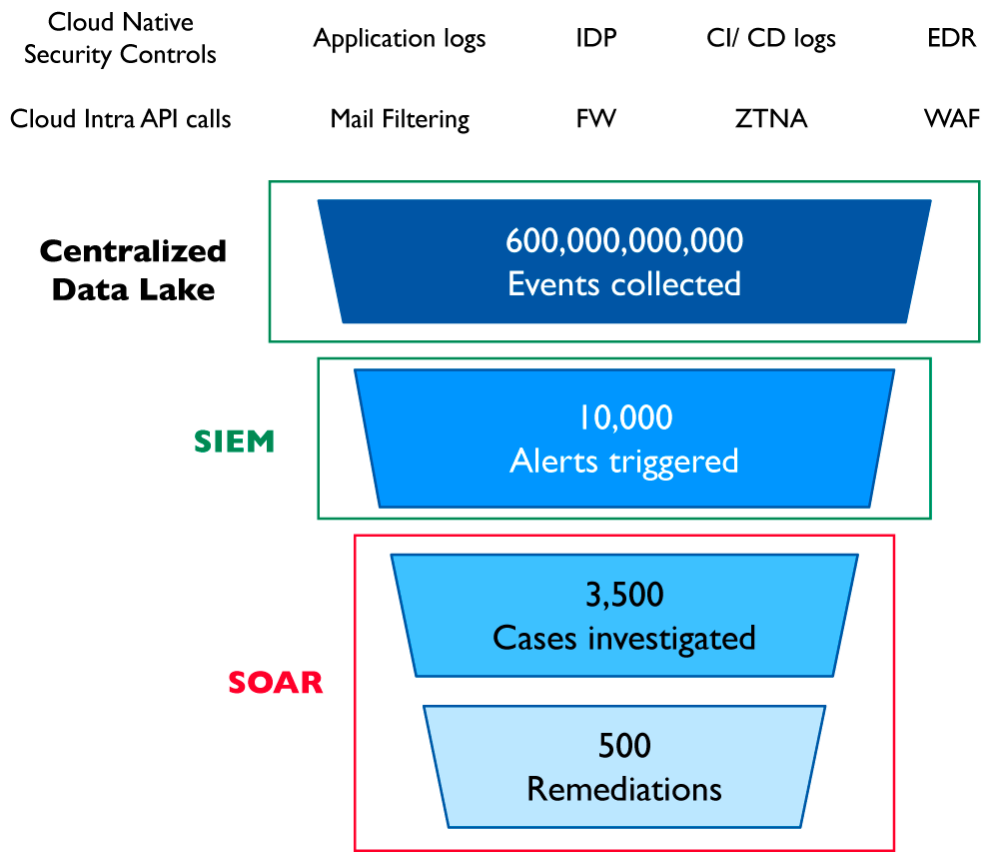


図3: モニタリングファネル

ソース： Microsoft Blog with additional info by Yaniv Menasherov's.

モニタリングファネルは、企業の検知および対応能力の進化を決定します。（テクノロジーで表される）各レイヤーは、セキュリティコンテキストを追加し、ノイズや誤検知を減らし、検知と対応能力を向上させます。

ファネルのトップゴールは以下です。

1. time-to-detect（TTD）の短縮
2. time-to-respond（TTR）の短縮
3. time-to-mitigate（TTM）の短縮

フェーズ1（インセプション）：IdP（アイデンティティプラットフォーム）、コラボレーションスイート、および利用している機密性の高いSaaSのモニタリングとイベントログをオンにしてください。ロギングを有効にするには、必ずしもシステム設定の問題ではなく適切なライセンスが必要な場合もあることに注意してください。

組織で5つ以上のシステムを使用している場合は、イミュータブルな集中型セキュリティデータレイクを作成し、ログソースを接続することをお勧めします。これにより、複数のシステムにログインする代わりに、1つの真のソースで簡単に調査を行うことができます。データを簡単にクエリし、電子メール、電話、またはSlackに基本的なアラートを作成できるようにします。このフェーズでは、企業のコラボレーションSaaSツールのログを取り込み、企業の電子メール、インスタントメッセージ（IM）、Fileshare Workspace（Office365またはGSuite）などのシステムを取り込む必要があります。さらに、これらのシステムの管理者監査ログ（admin audit log）が有効で、接続されていることを確認します。すべてのロギングに適切なSaaSライセンスがあることを確認してください。

フェーズ2（成熟期）：Security Information & Event Management （SIEM）ソリューションは、取り込まれたデータの相関関係を取り、正規化し、脅威インテリジェンスで強化することによって、セキュリティコンテキストを追加するために必要です。さらに、SIEMは、AWS/GCP/Azureにおける管理者認証など、既知のテクノロジーにおける既知のユースケースの本質的なモニタリングをサポートする、すぐに使える検出ルールを提供します。

フェーズ3（成長段階）：複数のイベントがインシデント（サイバー侵害など）に発展する前に、自動的にレスポンスできるSecurity Orchestration and Automation Response（SOAR）ソリューションが必要です。レスポンスは繊細で、適切に実行されないと本番環境にダメージを与えかねないため、これには多くのテーラーメイドのエンジニアリングが必要です。

下の図は、脅威のユースケース（赤）と、完全に成熟した企業がどのように情報を収集し、セキュリティコンテキストを追加し、アラートを作成し、自動応答を起動できるかの例です。

下のような本格的な規模になるには何年もかかります。しかし、上記のモニタリングファネルに従い、ここで説明した方法論を使うことで、以下を達成するためのマイルストーンを設定することができます。
青い点線の四角は上記の説明で、あなたのスタートアップのフェーズに合わせて完成させる必要があります。

どのように見えますか？

以下の図は、モニタリング、検知、および対応に関する赤（攻撃者）と青（組織のセキュリティオペレーション）を示しています。

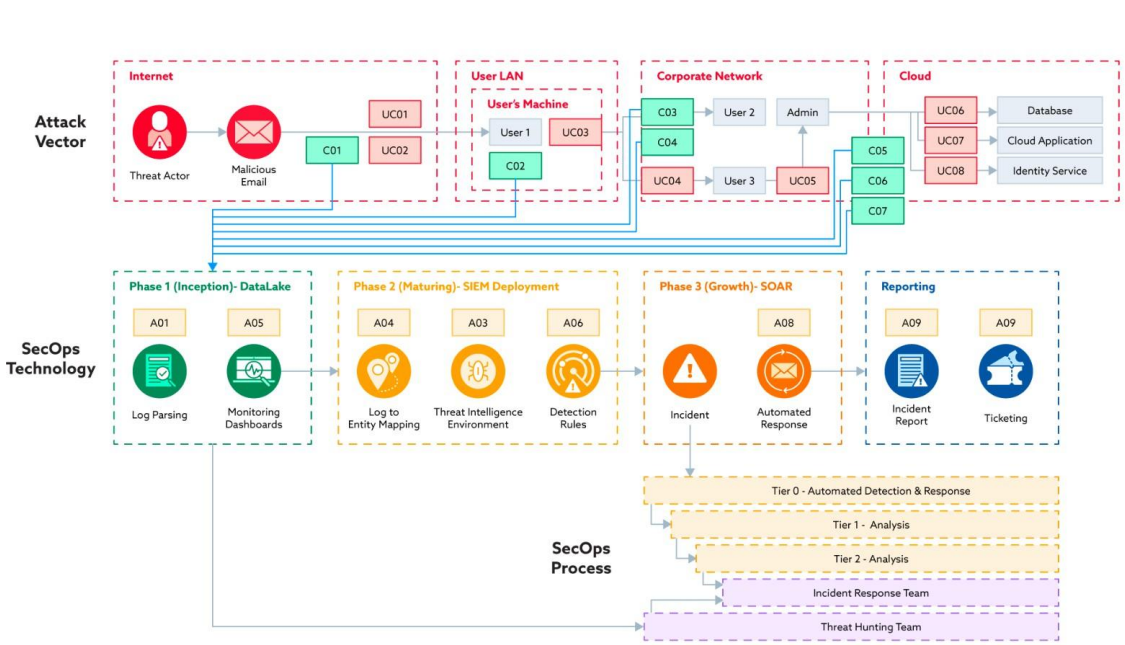
一番上の赤い行は、一般的な攻撃の攻撃ベクトルの例です：アカウントの乗っ取りを利用したデータの流出です。攻撃者は、各ステップとテクニックに UC0x（ユースケース）のフラグを付け、適切なセキュリティコントロール C0z によって監視できるようにします。

青い矢印は、さまざまなセキュリティコントロールからのログイベントを、単一の真の情報源であるイミュータブルなセキュリティデータレイクに取り込むことを表しています。

第2層は、セキュリティ運用の技術的側面を表します：セキュリティデータレイク > SIEM > SOAR。組織のステータスごとに、推奨されるSecOpsの技術を強調する異なる色がハイライトされていることに気づくでしょう。

- 緑色：フェーズ1、初期段階のスタートアップ企業向け
- 黄色：フェーズ2、成熟しつつあるスタートアップ企業
- オレンジ：フェーズ3、成長段階の組織

第3層は、セキュリティオペレーションセンター（SOC）、インシデントレスポンス（IR）、および脅威ハンティング（TH）チームなど、セキュリティオペレーションの人とプロセスの側面を表しています。次の章では、これらについて説明します。



Use Case (Attack Vector)	
ID	Description
UC01	Phishing + Spoofing
UC02	Email Containing Malware
UC03	Account Take Over
UC04	Lateral Movement
UC05	Privilege Escalation
UC06	Date Exfiltration
UC07	Critical Business Service Disruption
UC08	Persistency/ Domain Take Over

Security Controls	
ID	Description
C01	Email Protection
C02	Endpoint Detection & Response (AV & EDR)
C03	IDP/ IPS, F/W
C04	Identity Provider Audit Logs
C05	CSPM & CWPP
C06	CASB
C07	CloudTrail, VPC Flow, Route 53, Cloudwatch

SIEM SOAR SECOPS	
ID	Description
A01	Hot storage for logs
A03	External threat intelligence enrichment
A04	Correlation of entities and adding security context
A05	Monitoring dashboards
A06	Detection rules based threat scenarios creating incidents
A08	Automated response playbooks mechanism
A09	Ticketing and incident reporting within case management
T0	Automated detection, response and reporting
T1	Triage by SecOps Analyst
T2	Triage by internal IR Analyst

図4: アカウント乗っ取りによるデータ流出/ 業務妨害
ソース：Yaniv Menasherov, [Armada Security]

6.2.1 収集するログソース

次の表は、組織フェーズに合わせて収集するログのタイプとソースの詳細を示しています。また、収集したログソースの管理方法、推奨されるデータレイクタイプ、ログの保持ポリシー、ログの取り込みと収集のレビューを実行する頻度についても説明します。

最後に、この表は、どのフェーズでどのタイプの検出ルールを作成するかという点と、その利点を推奨しています。

1. **ルールベースの検出**：明示的なルールは、AWS root アカウントのログイン成功のような、特定の侵害の指標（IOC）やイベントを探します。
2. **適応ルール**：取り込まれたトラフィックに応じて自動的に調整され、セキュリティコントロールは適応的なメカニズムを提供します。
3. **行動分析のルール**：今日のセキュリティコントロールには、検出ルールに組み込まれたすぐに使える分析機能が搭載されるようになりました。これは、セキュリティコントロールの種類と購入ライセンスによります。

フェーズ	ログ内容	ログソース	ログ管理	イミュータブルなデータレイクストレージ
フェーズ1（インセプション）：	ユーザー認証や管理者認証、ネットワークアクセスなど、重要なシステムのロギングを有効にします。 ユーザーと管理者のログインと機密データへのアクセスをキャプチャします。	アイデンティティプロバイダー（IdP）、認証および認可ログ、企業コラボレーションツール（Microsoft 365、Google Workspace）	集中ロギングの実装 ログがイミュータブルであることを確認します。	AWS - S3 Azure - Log Analytics GCP - Google Cloud Storage (GCS)
フェーズ2（成熟期）：	クラウドAPIコール、データベースクエリ、ファイルアクセス、および詳細なユーザーアクティビティに拡張します。	クラウドサービス、SaaSアプリケーション、エンドポイントデバイス、およびネットワークアプライアンス。	ロールベースのアクセス制御を実装し、アクセスログを記録します。	SIEMソリューション： AWS - サードパーティのソリューションが必要です。AWS Security Lakeはまだ完全なSIEMソリューションではありません。 Azure - Microsoft Sentinel GCP - Chronicle
フェーズ3（成長段階）：	すべてのセキュリティコントロールイベントはログに記録されるべきです。	サードパーティサービス（SaaS）、人間以外のアイデンティティ、認証と認可、セキュリティコントロール、および高度な脅威検知システム。		サードパーティのSOARソリューションあるいはクラウドプロバイダーは、セキュリティイベントに対する自動応答を構築するために使用できる自動化サービスを提供しています。クラウドプロバイダーごとのサービス： AWS - Lambda/ Step function /SSM Azure - Logic Apps GCP - Google Security Operations SOAR マルチクラウドの状況をサポートするには、通常、サードパーティのソリューションの方が適しています。

フェーズ	ログの保持	ログレビュー	ルールベース	アダプティブ	ふるまい分析
フェーズ1（インセプション）：	コンプライアンスおよびインシデント調査のため、ログを少なくとも90日間保存します。	毎週レビューを実施し、自動化ツールを使用して異常をハイライトします。	ログインの失敗、機密データへのアクセス、およびシステムエラーのアラートを設定します。		
フェーズ2（成熟期）：	業界標準に準拠するため、ログは6〜12カ月間保存します。	ログは、セキュリティコンテキストを追加したイベントに要約されるべきです。 これはSIEMソリューションを使って行うことができます。イベントは毎日確認する必要があります（調査が必要ない場合はログを確認する必要はありません）。	SIEM OOTB（(Out-of-the-box（訳注：すぐに使える））ルールの活用。	コンテキストまたはリスク評価に基づいてログの冗長性を調整する適応型ロギング技術を実装します。	
フェーズ3（成長段階）：	規制要件に準拠し、フォレンジック調査をサポートするために、ログを数年間保持します。	インシデントやイベントのレビューを実施し、傾向を把握します。	OOTBがサポートできないカスタムメイドの検出ルールの作成	adaptive logging戦略をセキュリティ運用と完全に統合し、リアルタイムの脅威評価に基づいて動的に調整します。	AIがサポートするセキュリティコントロール行動分析エンジンを採用し、進化する脅威や組織の変化に基づいてモデルを改良します。 セキュリティコントロールは、コンテキストのない生のログの代わりにイベントを取り込むことができます。

6.3 インシデントレスポンス

このセクションでは、クラウドベースのスタートアップ企業が上記の3つのフェーズで考慮すべき重要なセキュリティ面の概要を説明します。各フェーズには固有の課題があり、セキュリティ成熟度に合わせたアプローチが必要です。

一般的には以下になります。

- **パニックにならないでください！**規模の大小にかかわらず、すべての組織はサイバー攻撃に脆弱です。
- **データ侵害**：機密性の高い顧客データへの不正アクセスにより、財務上の損失、風評被害、および規制当局による罰金などが発生します。
- **ランサムウェア攻撃**：重要なデータを暗号化し、復号の代金を要求することで、業務に支障を与え、経済的損失をもたらします。
- **サービス拒否（DoS）攻撃**：インフラストラクチャをトラフィックで圧倒し、正規のユーザーがサービスを利用できないようにします。

被害を最小限に抑え、効果的に復旧するためには、冷静さを保ち、計画的な対応計画を立てることが重要です。

6.3.1 準備

フェーズ1（インセプション）：

- **基本的なインシデントレスポンスポリシー**：セキュリティインシデントを特定し、報告し、対応するためのわかりやすいプロセスを定義します。これは、役割、責任、およびコミュニケーションチャネルを概説した簡単な文書でも構いません。

- **基本的な検出と識別**：基本的なセキュリティモニタリングツールを導入し、不審なアクティビティ（ログインの失敗や異常なネットワークトラフィックなど）を検出します。

助言：Fail2banや Suricataのようなオープンソースの検知ソリューションを検討してください。Fail2banは、ログイン試行が何度も失敗した場合にIPアドレスをブロックし、Suricataは、不審なアクティビティがないかネットワークトラフィックをモニタリングすることで侵入を検知します。

- **まずアイデンティティ認証と認可をコントロールします。**クラウドベースのIDPは、IAMアクティビティに関する優れた可視性を備えています。また、基本的な可視性を得るために大規模なエンジニアリングが必要なオンプレミスのIDPとは異なり、基本的なアラートを電子メールで直接作成することができます。
- **内部通知**：CTO、ITチーム、CEOなどの重要人物を含め、インシデント通知のための明確な指揮系統を確立します。

フェーズ2（成熟期）：

- **正式なインシデントレスポンスポリシー**：業界のベストプラクティス（SANS、NISTなど）に沿った包括的なポリシーを策定します。エスカレーション手順、データ侵害通知要件、および外部コミュニケーション戦略を含みます。ガイダンスについては、NIST サイバーセキュリティフレームワーク （CSF）を参照してください。
- **高度な検出と識別**：相関機能を備えた高度なセキュリティモニタリングツール（SIEM、EDRなど）を導入 し、インシデントをより効果的に検出して調査することができるようにします。詳細は、本書第5章のデバイスコントロールと第2章のワークロード管理を参照してください。
- **外部通知のコミットメント**：データセキュリティインシデント（DSI）手順を作成し、情報漏えいが発生した場合に外部の利害関係者（顧客、規制当局など）に通知するトリガーとタイムラインを定義します。また、役割、意思決定者、およびDPOのほか、規制当局が要求する対象者ごとの漏えい記録数の算出方法も記載します。

助言：データ保護規制（EUのGDPRやカリフォルニア州のCPRAなど）には、違反通知の義務に関する厳しい規則があります。データ侵害通知の要件については、関連するデータ保護（DP）規則を確認してください。

- **対応手順**：リスクレジストリで特定された脅威、または業界ベクトルに関連する脅威に対応するさまざまなインシデントシナリオに基づいて、詳細な封じ込め、根絶、およびリカバリ手順を策定します。
- **インシデントレスポンス（IR）リテイナー外部当事者契約**：インシデントレスポンス（IR）チームまたはITセキュリティコンサルタントと契約を締結し、専門的なサ ポートを受けることができるようにします。
- **サイバー保険**：侵害に関連する財務リスクを軽減するためのサイバー保険のオプションを検討します。サイバーリスク専門の保険ブローカーに相談します。
- **リクルート**：最初のクラウドサイバーセキュリティ検知対応エンジニアを獲得してください。クラウドサービス全体の可視性を高め、対応能力を維持する方法を計画する時です。

フェーズ3（成長段階）：

- **リクルート**：2人目、3人目のクラウドサイバーセキュリティ検知および対応エンジニアを獲得してください。規模を拡大するにつれて、クラウドセキュリティの専門家は開発チームと協力して、アプリのアーキテクチャとカスタムアプリのログを理解する必要があります。
- **定期的なIRエクササイズ**：社内外の関係者（ R&D 、コンサルタント、法務、およびフォレンジック専門家）が参加するインシデント対応シミュレーションを定期的に実施し、対応計画をテストし、改善します。机上演習や実戦訓練を検討します。
- **継続的な改善**：演習や実際のインシデントから学んだ教訓に基づき、インシデント対応計画を定期的に見直し、更新します。

6.3.2 インシデントの封じ込め

フェーズ1（インセプション）：

- **基本的な封じ込め**：侵害されたシステムの隔離や侵害されたアカウントの無効化など、インシデントの拡大を阻止するための迅速な対応に注力します。
    - **シナリオ**：あるスタートアップ企業が、悪意のあるリンクで従業員を標的にしたフィッシングキャンペーンを検知しました。早急な封じ込めには、疑わしいリンクを無効にし、従業員のパスワードをリセットすることが必要です。
      IdPとSaaSアプリケーションの管理ポータルを通じて「セッションの失効」をプッシュし、即座にアクセスを失効させます。パスワードのリセットやアカウントの無効化は、攻撃者側で認証トークンを24時間有効にしておく可能性があることを理解することが重要です（失効が実行されない場合）。
- **基本的な根絶**：インシデントの根本原因（マルウェア、設定ミスなど）を特定し、除去します。特定された危険なエンティティをすべて同時に削除することが不可欠です。「キルスイッチ」と呼ばれるこのアクションは、攻撃者が足場を固めていることに気づかれる前に、その足場をすべて破壊します。徐々にそれらを削除すると、攻撃者は気づき、より攻撃的になります。
    - **シナリオ**：フィッシングキャンペーンの後、スタートアップ企業は侵害された従業員アカウントを侵入口として特定します。根絶には、攻撃者の追放、アカウントのセキュリティの確保、および強固なパスワードポリシーの実施が必要です。5つのアカウントが特定され、パスワードのローテーションが行われ、同時期にアクセスが取り消されました。
- **基本的なリカバリ**：影響を受けたシステムとデータをバックアップから復元します。
    - **シナリオ**：フィッシング攻撃でデータが漏えいした場合、スタートアップ企業はバックアップから該当するデータを復元し、今後同様のインシデントを防ぐために追加のセキュリティ対策を実施します。
- **社内コミュニケーション**：インシデントと対応策について社内の利害関係者に情報を提供します。
    - **シナリオ**：このスタートアップ企業のCEOとITチームは、フィッシング攻撃、対応策、および今後同様のインシデントを防ぐための手順について、従業員と透明性のあるコミュニケーションをとります。

フェーズ2（成熟期）：

- **包括的な封じ込め計画の策定と維持**：詳細な手順書と自動化されたレスポンスプレイブックを含みます。
- **分離とセグメンテーション**：侵害されたシステムまたはネットワークセグメントを迅速に分離するためのネットワークセグメンテーション機能を確立します。
- デバイスの信頼性を確立することは簡単なことではありません。しかし、一度実現すれば、侵害されたエンティティを「信用しない」ことで、実際のインシデント中にアイデンティティ、ネットワーク、およびデバイス全体で脅威に対応し、封じ込め、および根絶することは非常に簡単で

す。

- **Infrastructure as Code（IaC）**：IaCの原則を統合し、クリーンなインフラストラクチャの迅速な再展開と、バックアップやスナップショットからの合理的なリカバリを可能にします。これにより、手作業による介入を減らし、封じ込めプロセスをスピードアップすることができます。
- **セキュアなデータバックアップ**：データの完全性と復元時の可用性を確保するため、セキュアなストレージと定期的なテストにより、正確でイミュータブルなバックアップ戦略を確立します。

6.3.3 インシデント管理

フェーズ1（インセプション）：

- **基盤の設定**：
  - 資産と重要度のマッピング
  - 封じ込め手順の理解
  - ログとアラートのソースをマッピング
  - 災害復旧の基盤を構築 - IACを使用して構成と設定をキャプチャし、異なる/保護された場所にデータの分離されたコピーを作成（災害復旧の詳細については、第2章を参照してください）

フェーズ2（成熟期）：

- **正式な封じ込め手順**：インシデントの種類と重大性に基づき、封じ込めのための文書化された手順を実施します。これらの手順では、侵害されたシステムやネットワークの隔離のような具体的なアクションの概要を説明する必要があります。
  - 侵害されたアカウントの無効化
  - アクセス権限の剥奪
  - 機密データの保護
  - フォレンジック捜査のための証拠保全
- **脅威ハンティングとフォレンジック**：高度な脅威ハンティング技術とフォレンジック分析により、攻撃者の痕跡をすべて特定し除去します。これには以下が含まれます：
  - ログやネットワークトラフィックを分析し、不審なアクティビティを検出
  - 侵害の指標（IOC）を特定
  - システム内での攻撃者の動きを追跡
  - フォレンジック証拠の収集と分析
  - クラウドで脅威ハンティングを行う最大の利点は、クラウドプロバイダーが関連ログを集約する簡単な方法を提供し（Enabler）、クラウド/データレイク上の組み込みSIEMにOOTB脅威ハンティングクエリを起動するツールを提供し（How）、最後に、同じクラウドプロバイダーを利用している他の利用者に対するグローバルな攻撃に基づく、貴重な脅威インテリジェンスを得ることができます。
- **災害復旧計画**：大規模な障害やデータ損失から迅速にリカバリできるよう、包括的な災害復旧計

画を実装します。この計画には以下が含まれます：

- バックアップとリカバリ手順
- 事業継続とダウンタイム緩和戦略
- 利害関係者に通知するためのコミュニケーション計画
- 計画の定期的なテストと実行

フェーズ3（成長段階）：

- **自動レスポンス**：ダウンタイムと影響を最小限に抑えるために、特定の封じ込めおよびリカバリ活動を自動化します。これには以下が含まれます。
  - 侵害されたシステムの自動隔離
  - 影響を受けたアカウントのパスワードの自動リセット
  - セキュリティパッチの自動デプロイメント
- **机上エクササイズ**：複雑な事故シナリオをシミュレートした机上演習を実施し、プレッシャーのかかる状況で対応計画をテストします。このような演習には、関係するすべての利害関係者が参加し、改善が必要な部分を特定するために役立ちます。

6.3.4 教訓

フェーズ1（インセプション）：

- **基本的な報告**：時系列、影響、学んだ教訓など、インシデントの詳細を文書化します。
- **初期修復**：影響を受けたシステムとデータを使用可能な状態に復元します。

フェーズ2（成熟期）：

- **詳細な報告**：インシデントの根本原因、範囲、および影響を理解するための徹底的な調査を行います。実行可能な推奨事項を記載した正式な報告書を作成します。
- **根本原因の分析**：インシデントを分析し、侵害につながった根本的な脆弱性を特定して対処します。これには以下が含まれます。
  - システムログと設定のレビュー
  - セキュリティ上の弱点の特定
  - 脆弱性評価の実施
  - 具体的な事後処理を作成し、セキュリティを向上させ、再発の可能性を減らします。

フェーズ3（成長段階）：

- **教訓の共有**：インシデントから学んだ教訓を関連チームと共有し、全体的なセキュリティポスチャを改善します。これは、社内のトレーニングセッション、ナレッジベースの記事、またはセキュリティ意識向上キャンペーンを通じて行うことができます。
- **セキュリティ意識向上トレーニング**：セキュリティの脅威とベストプラクティスに対する従業員の意識を高めるため、定期的なセキュリティ意識向上トレーニングを実施します。不審な行動を特定し報告する権限を従業員に与えることで、将来の事故を防ぐことができます。

6.4 章のサマリー

	フェーズ1	フェーズ2	フェーズ3
方法論 &テクノロジー	基本的なログソースをオンにして収集を開始	SIEMやデータレイクなどのログ管理ソリューションの導入。 ログソースを追加。	SOARのレイヤーを追加。 ログ保存ポリシーの導入、ふるまいエンジンの追加
インシデントレスポンス	認証イベントに焦点を当てた基本ポリシー	正式な方針、通知、および報告手続き。 成熟したバックアップとIACの昇格、脅威ハンティングシナリオの開始	インシデント対応エンジニアの採用、またはサードパーティの利用。定期的な練習と改善。自動応答の追加

7. その他考察

7.1 SaaSベースのスタートアップとAI

人工知能（AI）はSaaSスタートアップにとって重要なツールです。しかし、AIソリューションを成功させるには、膨大なコンピューティングパワーとデータストレージが必要です。そのためにはCSPとの連携が不可欠です。

CSPは、高性能なコンピューティングリソースや膨大なデータストレージ容量など、堅牢なクラウドインフラストラクチャーを提供します。適切なCSPの専門知識とインフラストラクチャを活用することで、スタートアップ企業は中核となる開発タスクに集中し、革新的なAI搭載ソリューションで市場投入までの時間を短縮することができます。

セキュリティ脅威の検出： SaaSスタートアップ企業は、CSPのインフラを活用し、AIを使用して広範なデータセットを分析することで、異常や疑わしい活動を特定し、セキュリティ上の脅威をリアルタイムで早期に検知・防止することができます。

ユーザー行動分析（UBA）：AIアルゴリズムはユーザーの行動を分析し、内部脅威や侵害されたアカウントを検出することができます。これらの洞察により、よりプロアクティブなセキュリティポスチャが可能になります。

脆弱性管理：AI主導のツールが脆弱性のスキャンと優先順位付けを合理化します。これにより、スタートアップ企業はセキュリティ課題に迅速に対処することができます。このように優先順位付けを重視することで、リソースが効率的に配分されるようになります。

自動化されたセキュリティインシデントレスポンス：インシデントレスポンスプロセスにAIを組み込むことで、封じ込めや修復作業などの重要なタスクを自動化することができます。この自動化によって対応時間が短縮され、セキュリティインシデントの潜在的な影響が大幅に軽減されます。

セキュリティ自動化：AIは定型的なセキュリティ業務を自動化することで、セキュリティ要員を高度な計画や脅威分析など他の業務に集中させることができます。

データの質：AIモデルの有効性は、基礎となるデータの質と連動します。データが正確かつ包括的であることが、AIを活用した効果的なセキュリティソリューションを可能にします。

説明可能性と透明性：意思決定プロセスを理解し、意思決定の方法を透明化することで、AI主導の行動が公正で偏りのないものになります。

専門知識：AIセキュリティソリューションの導入と管理には、専門的な知識とスキルが必要です。組織はこの専門知識を社内で開発するか、外部との提携を模索する必要があります。

詳細は以下を参照してください。
@ AI Safety Initiative
@ AI Technology and Risk | CSA
@ AI Governance & Compliance | CSA @ AI Controls | CSA
@ AI Organizational Responsibilities | CSA

7.2 SaaSベースのスタートアップとゼロトラスト

SaaSベースのスタートアップ企業は、クラウドベースでサービスを提供し、多様な、おそらくはグローバルなユーザーベースを持つため、堅牢で適応性のあるセキュリティフレームワークが必要です。ゼロトラスト（ZT）は、「信用せず、常に検証する」という基本原則を掲げており、SaaSベースのスタートアップ企業のニーズに完全に合致しています。

分散した労働力とリソース：リモートチームとクラウドインフラストラクチャーを持つSaaSベースのスタートアップ企業は、最小特権アクセスと継続的検証を重視するゼロトラストのメリットを享受できます。

より強固なセキュリティのためのコラボレーション：多くのCSPは、多要素認証（MFA）やきめ細かなアクセス制御など、ゼロトラストの原則をサポートするセキュリティ機能を提供しています。ゼロトラストを優先するCSPと協力することで、スタートアップ企業は自社の環境をセキュアにする貴重なパートナーを得ることができます。

インフラストラクチャではなくイノベーションに注力：CSPは、ゼロトラストが要求するインフラストラクチャとセキュリティの専門知識を提供します。これにより、SaaSベースのスタートアップ企業は中核となる開発業務に専念できるようになり、革新的なソリューションの市場投入までの時間が短縮されます。

クラウドアライメント：SaaSベースのスタートアップ企業はクラウドベースのインフラストラクチャで運営されており、ゼロトラストアーキテクチャ（ZTA）はこれらの環境と統合されています。この統合により、セキュリティはクラウドサービスとともに進化します。

ダイナミックなユーザーベース：SaaS ベースのスタートアップ企業は通常、広範かつダイナミックなユーザーベースにサービスを提供しているため、従来の境界ベースのセキュリティモデルでは不十分です。ゼロトラストは、発信元を問わずすべてのアクセス要求を検証することに重点を置いており、SaaSプラットフォームがセキュアにアクセスを管理するために必要です。

拡張性と柔軟性：SaaSベースのスタートアップ企業が規模を拡大するにつれて、そのセキュリティフレームワークは、効率性や有効性を損なうことなく適応できる必要があります。マイクロセグメンテーションと最小特権を使用するゼロトラストのセキュリティへのアプローチは、スタートアップ企業とともに成長できるスケーラブルなセキュリティを可能にします。

アイデンティティとアクセス管理（IAM）の強化：SaaSベースの企業にとって、MFAや役割ベースのアクセ

ス制御（RBAC）を含む堅牢なIAM機能は、セキュアなスケーリングとユーザー管理をサポートするために必要な基礎的要素です。

継続的なモニタリングと分析: SaaSベースのスタートアップ企業が提供するサービスでは、アクセス要求とユーザー活動を継続的にモニタリングする必要があります。高度なアナリティクスとAIによる脅威検知を導入することで、SaaSベースのスタートアップ企業にリアルタイムの洞察とプロアクティブな脅威の緩和を提供することができます。

効率化のためのシームレスな自動化：自動化により、SaaSベースのスタートアップ企業はセキュリティを確保しながらイノベーションを起こすことができます。自動化により、検証とセキュリティ対応アクションを合理化し、進化するユーザーの役割とコンテキストに基づくアクセス権をサポートします。

ゼロトラストモデルを採用することで、SaaSベースのスタートアップ企業は、セキュリティがボトルネックではなく、成長とイノベーションの促進要因となることを確実にし、SaaSベースのスタートアップ企業が競争の激しいデジタルエコシステムで成功することを可能にします。

詳細はこちらへ：Zero Trust Advancement Center

6.1 SaaSスタートアップと量子コンピューティング

量子コンピューティングは変革をもたらす技術です。SaaSベースのスタートアップ企業にとって、量子コンピューティングは運用、製品提供、および脅威に対するデータセキュリティに影響を与えます。しかし、この可能性を引き出すには、CSPとの協力が必要です。

量子インフラストラクチャへのアクセス：量子ハードウェアの構築と維持は、SaaSベースのスタートアップ企業には不可能な大仕事です。これらのリソースへのアクセスを積極的に構築または統合しているCSPと協力することで、SaaSベースのスタートアップ企業がこのテクノロジーにアクセスできるようになります。

量子の専門知識とツール：CSPは量子の専門知識に投資し、量子資源へのアクセスと活用のためのユーザーフレンドリーなツールを開発することが期待されています。これにより、社内に量子の専門家がいない新しいスタートアップ企業でも、これらのソリューションを検討し、統合することができます。

量子時代のセキュリティ：量子コンピューティングが進歩すると、現在の暗号標準は脆弱になります。量子セキュリティを優先するCSPと提携することで、この新時代においてもサービスのセキュリティを確保することができます。

イノベーションと製品開発の加速：この加速は、特に創薬、財務モデリング、および複雑なシステムシミュレーションなどの革新的な製品やサービスの開発につながり、SaaSベースのスタートアップ企業に競争力をもたらします。

セキュリティを強化する耐量子暗号：量子コンピュータは、今日のインターネットやクラウドサービスをセキュアにしている暗号プロトコルの多くを破ることができます。したがって、SaaSベースのスタートアップ企業は、将来の量子攻撃から保護するために耐量子暗号を組み込む必要があります。

最適化と効率化：量子コンピューティングは、ロジスティクス、サプライチェーン管理、および資源配分の最適化に新たな可能性をもたらします。SaaSベースのスタートアップ企業は、量子アルゴリズムを活用して、運用を最適化し、コストを削減し、サービス効率を向上させることができます。

量子リテラシーとスキル開発：SaaSベースのスタートアップ企業は、量子リテラシーとスキル開発に投資する必要があります。量子コンピューティングの原理を理解し、量子技術の発展に遅れをとらないことが、その利点を活用し、量子ソリューションを統合する上で極めて重要です。

量子テクノロジープロバイダーとのコラボレーション：量子テクノロジープロバイダーとのパートナーシップや量子コンピューティングエコシステムへの参加により、SaaSベースのスタートアップ企業は量子コンピューティングのリソースや専門知識を利用することができます。

耐量子セキュリティ対策の早期導入：量子コンピューティングがもたらすセキュリティの課題を予見し、SaaSベースのスタートアップ企業は、セキュリティアーキテクチャに耐量子暗号アルゴリズムを統合することを優先すべきです。

量子対応インフラストラクチャへの戦略的投資：量子コンピューティングの進化に伴い、SaaSベースのスタートアップ企業は、自社の技術インフラストラクチャに対する長期的な影響を考慮する必要があります。量子力学に対応したソリューションやプラットフォームに投資することで、スタートアップ企業が商業的に存続できるようになります。

量子コンピューティングは、SaaSベースのスタートアップ企業にチャンスと課題の両方をもたらします。この新たなテクノロジーを取り入れることで、スタートアップ企業は製品の革新とセキュリティの向上を実現することができます。

詳細はこちらへ：Cloud Security Allianance Working Group Site

7. 参考文献

Sqreen, The SaaS CTO Security Checklist
https://s3-eu-west-1.amazonaws.com/sqreen-assets/whitepapers/SaaS+CTO+Security+Checklist.pdf

Github, Security-101-for-saas-startups
https://github.com/forter/security-101-for-saas-startups/blob/english/security.md

Fast Company, 7 factors to consider before implementing AI in your SaaS company, Amanda Yello and Metin Kortak, March 2024
https://www.fastcompany.com/91057043/7-factors-to-consider-before-implementing-ai-in-your-saas-company

NxtStep, Unlocking The Benefits Of Artificial Intelligence SaaS In 2023, Sean Boyce, September 2023,
https://nxtstep.io/blog/artificial-intelligence-saas/

HCLTech, Leveraging AI to revolutionize SaaS businesses, Jordan Smith, September 2023,
https://www.hcltech.com/trends-and-insights/leveraging-ai-revolutionize-saas-businesses

Cloudflare, Zero Trust controls for your SaaS applications, August 2021
https://blog.cloudflare.com/access-saas-integrations/

Cloudflare, Zero Trust controls for startups
https://developers.cloudflare.com/reference-architecture/design-guides/zero-trust-for-startups/

Microsoft, Integrate SaaS apps for Zero Trust with Microsoft 365, October 2023
https://learn.microsoft.com/en-us/security/zero-trust/integrate-saas-apps

DoControl, Zero Trust Data Access (ZTDA), Extend Zero Trust to the SaaS Application Data Layer, March 2024, https://www.docontrol.io/zero-trust-data-access

Cutting Edge Circuit, Exploring the Potential of Quantum Computing in SaaS Solutions, March 2024
https://cuttingedgecircuit.com/exploring-the-potential-of-quantum-computing-in-saas-solutions

Seskir, Z.C., Korkmaz, R. & Aydinoglu, A.U.The landscape of the quantum start-up ecosystem.EPJ Quantum Technol.9, 27 (2022). https://doi.org/10.1140/epjqt/s40507-022-00146-x

The Quantum Insider, 73 Quantum Computing Startups Challenging Industry Leaders, James Dargan, May 2023
https://thequantuminsider.com/2023/05/09/quantum-computing-startups/

Appendix A:インシデントレスポンスのための実践ガイド

1. 芝を知る：資産と責任のマッピング

- クラウドインベントリーテンプレート
  - リソース名：(例："Production Database")
  - リソースタイプ: (例: AWS RDS、Azure SQL Server など)
  - 目的：（「顧客の注文情報を保存する」など）
  - データの機密性：（例：高 - クレジットカード番号を含む）
  - 接続：（「グループXのウェブサーバーがこのデータベースにアクセスする」など）
- **責任分担表**：
  - リソース名(インベントリと一致)
  - 主な所有者：(技術担当者の氏名と連絡先)
  - エスカレーション：(オーナーが不在なら、次は誰？)

指示：これは*ライブ文書*であることを強調します。スタートアップがクラウドリソースを追加または変更する際には、定期的な更新が必要です。

2. ツールキットの準備：セキュリティに不可欠な武器

- ロギングとモニタリング：
  - **エッセンシャルログ**：
    - オペレーティングシステムのイベントログ
    - クラウドプロバイダーのセキュリティログ（AWS CloudTrailなど）
    - アプリケーション/ウェブサーバーのアクセスログ
    - ネットワークファイアウォールのログ
    - IDP認証、認可、およびIAMログ
    - CASBログ - アカウントアクティビティログ
  - **集中化**：
    - 推奨ツール：ELK Stack、Splunk、クラウドプロバイダーの同等の製品
    - ワークフロー：提案するツールの基本的なログ転送設定を説明
- アラート：
  - トップ5の優先事項：
    - 通常とは異なる場所からの複数のログイン失敗
    - 通常営業時間外のデータアクセスの急増
    - クラウド資産の予期せぬ構成変更
    - 異常な送信ネットワークトラフィックパターン

        - アンチウイルス/アンチマルウェアソフトウェアからの警告
    - **誤検知**：
        - その理由を簡単に説明
        - 推奨：大まかなアラートから始め、システムの「通常」の動作を知るにつれて、徐々にアラートを絞り込んでいきます。
- **脆弱性のスキャン**：
    - **ツール**：予算に余裕があれば、オープンソース（OpenVAS、Nessus）と商用オプションを提案します。
    - **修復ワークフロー**：
        - 所見に対する重大度の割り当て（Critical、Highなど）
        - 各重大度レベルを修正するための時間枠を定義（例：クリティカル（Critical）の場合は24時間以内）。
        - これを責任分担表に結びつけます - パッチ適用サーバーの管理、アプリケーションの更新などは誰が担当しますか？

3. ヒューマンファクター：チームと教育

- **"非セキュリティ" スタッフ**
    - **何を報告すべきか**：
        - フィッシングメール（例を挙げる）
        - 予期せぬシステムのスローダウンやクラッシュ
        - 異常なポップアップやエラーメッセージ
        - 「不適切」と思われる機密データの要求
    - **報告のメカニズム**：メールアドレス、ウェブフォームなど。*簡単化します。*
    - **非難しない文化**：「何か見つけたら、何か言う」ことは、罰せられるのではなく、賞賛されるべきです。
- **チーム間のコミュニケーション**：
    - **事故前の連絡先リスト - 役割の例を含めます**：
        - CTO/IT部門長
        - CEO
        - 法務責任者（スタートアップが小規模の場合は外部の弁護士）
        - カスタマーサポート/PR責任者（違反が顧客に影響を及ぼす可能性がある場合）

4. 計画を持つ（なぜなら、パニックは敵）

- **インシデントレスポンスの詳細**
    - **早急な対応**
        - **[ ]** 侵害されたシステムを隔離；スタートアップのクラウド設定に関連する指示を提供します。
        - **[ ]** 漏洩した可能性のあるパスワードの変更

        - [ ] スナップショット／フォレンジックのイメージを取ります（可能な場合）
    - **連絡先リスト:**インシデント発生前のリストを使用。必要に応じて他のリストを追加できるスペースを確保。
    - **文書化**：
        - [ ] 最初の警告のタイムスタンプ
        - [ ] 影響を受けたシステム
        - [ ] これまでの取り組み
        - [ ] インシデント前／インシデント中の異常な観察事項
- **机上エクササイズ**：
  シナリオ：最初はシンプルに（フィッシング攻撃、ランサムウェア）、後で複雑化
    - **ゴール**：誰が "勝つか "ではなく、この練習でどのようなギャップが明らかになったかが重要です（例：コミュニケーションの断絶、不足しているツールなど）。

Appendix B:サイバー攻撃ウォークスルー

このセクションでは、実際のインシデントとそこから学んだ重要な教訓を中心に、注目すべきサイバー攻撃のウォークスルーを提供します。このような攻撃を調査することで、スタートアップ企業は効果的な防御策や対応策に関する洞察を得ることができます。

SolarWindsサイバー攻撃

概要：SolarWindsの情報漏洩事件は、デジタルサプライチェーンの脆弱性を浮き彫りにしました。攻撃者は、多くの組織にアクセスするために信頼できるベンダーを侵害し、偵察とネットワーク全体のラテラルムーブメントに重点を置きました。

教訓：

- デジタルサプライチェーンのセキュリティ確保とネットワーク行動のモニタリングの重要性。
- 厳密なコード監査と検証プロセスは非常に重要です。
- 振る舞い検知を含む高度な脅威検知メカニズムは、プロセスの名目上の信頼性に関係なく、悪意のある活動を特定するために不可欠です（SentinelOne）。

NotPetyaマルウェア

概要：当初、ランサムウェアを装ったNotPetyaは、広範囲に混乱を引き起こすことを目的としていました。この世界的な攻撃は、Microsoft Windowsの脆弱性をエクスプロイトしたもので、さまざまな分野に影響を与え、100億ドル以上の損害をもたらしました。

教訓：

- このインシデントは、強固な脆弱性管理と多層的なサイバーセキュリティ防御の導入の必要性を浮き彫りにしました。
- サイバーツールの破壊的な可能性と、サイバーセキュリティにおける世界的な協力の重要性を強調しました（SentinelOne）。

WannaCryランサムウェア攻撃

概要：150カ国で20万台以上のコンピュータに影響を与えたWannaCryは、Microsoft Windowsの重大な脆弱性をエクスプロイトしました。その急速な広がりと多くの部門への影響は、パッチが適用されていないシステムの脆弱性を浮き彫りにしました。

教訓：

- この攻撃は、タイムリーなシステム更新と既知の脆弱性へのパッチ適用の必要性を強調するものでした。
- サイバー脅威の世界的な広がりと無差別性を実証し、包括的なサイバーセキュリティ対策の必要性を浮き彫りにしました（SentinelOne）。

Optus侵害

概要：オーストラリアの人口の約40%が影響を受けたOptus侵害は、認証なしでアクセスを許可するAPIが原因だったと報告されています。このミスは、インターネットでアクセスできる実際のデータをテスト環境に置いたことによる、人間の見落としによるものです。

教訓：

- APIを保護し、堅牢な認証メカニズムをセキュアにすることの重要性。
- ヒューマンエラーはサイバーセキュリティに大きな影響を与える可能性があり、厳格なテスト環境とデータ保護プロトコルの必要性が強調されています（ISACA）。

Automated Libra Campaign

概要：Automated Libra Campaignでは、Captcha実装の弱点をエクスプロイトし、自動化を用いてクラウドプロバイダー上に数千のアカウントを作成しました。この巧妙な操作は、悪意のある目的のためにCI/CD技術を使用することを強調しました。

教訓：

- 自動化された攻撃に対するセキュリティ対策を強化する必要があります。
- 攻撃者が使用する高度なCI/CDおよび自動化技術に対抗するためのセキュリティプロトコルの継続的な改良と改善（BCS）。

LastPass Breach

概要：LastPassが暗号化されたデータにアクセスされる事件が発生しました。この事件は、強固なマスターパスワードに依存しているにもかかわらず、クラウドサービス上に機密データを保存する脆弱性を明らかにしました。

教訓：

- 強固な暗号化であっても、特にマスターパスワードが脆弱であれば、攻撃を受ける可能性があります。
- 機密性の高いデータの保存には、クラウドストレージよりもセキュアな方法が必要な場合があり、パーソナルコンピューティングリソース（BCS）のコントロールが重視されます。

これらのインシデントは、進化するサイバー脅威の性質と、サイバーセキュリティに対する積極的かつ包括的なアプローチの必要性について、貴重な洞察を与えてくれます。このような実際の攻撃から学ぶことで、スタートアップ企業は潜在的なサイバーインシデントに対する準備とレジリエンスを強化することができます。