ASCJ クラウドセキュリティ ガイダンス&ベストプラクティス

AWS 環境における クラウドセキュリティへの 取り組み方

1.0 版

APN セキュリティコンソーシアム・ジャパン

目次

1 背景

エンタープライズ領域でクラウドが利用され 10 年ほど経ち、今日、企業におけるシステム構築では、資産管理、メンテナンス、導入コスト、リソース弾力性の面でオンプレミスより有利なクラウドの採用が進んでいる。

しかしながら、クラウドに任せる箇所と、自ら考えて設計する箇所を意識せずにシステムを構築していては、セキュリティ部分で問題が発生しがちである。適切な設計と運用がなされず、結果、クラウド上に保管した機密情報が漏洩した事故が多数発生している（注 1）。ストレージやデータベースをクラウドへ移行したが、セキュリティの設定が十分ではなく、機密情報をインターネットに公開してしまい、多数の顧客情報や個人情報を漏洩させてしまったケースがある。これらはクラウド自体に原因があったのではなく、クラウドを使いこなせなかった利用者側に原因がある。また、クラウドを使いこなす技術のみならず、経営側にもシステムを監査するコンプライアンス対応への意識が欠落していた可能性が高い。

適切なセキュリティ対策を施して、システムを運用するには、クラウド利用の前提である、責任分界点やサービス内容の理解が必要である。この理解はシステムを構築する SIer 企業のみならず、クラウドを利用してサービスを提供するユーザー企業にも必要なものである。

事故を回避するために、情報セキュリティ基準があり、その適用が提言されている。日本国では「政府機関等の情報セキュリティ対策のための統一基準（注 2）」「経済産業省情報セキュリティ管理規程（注 3）」「経済産業省情報セキュリティ対策基準（注 4）」などがあり、最近では、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、クラウドサービスの円滑な導入を目的とした制度である「政府情報システムのためのセキュリティ評価制度（ISMAP）（注 5）」も公開された。また、システムの特性によっては、日本国外の基準やリファレンスへの適応が必須な場合がある。基準には、欧州ネットワーク情報セキュリティ庁（ENISA）（注 6）や Cloud Control Matrix（CCM）（注 7）のようなガイドラインが該当する。さらに、国際的な対応だけでなく、ドメインに特化した、金融機関向けの「FISC 安全対策基準（注 8）」や、医療機関向けの「3 省 3 ガイドライン（注 9）」もある。

これらの基準は対策範囲が広いため、内容を読み解き、クラウドへ適用するには相当の知識とスキルが必要である。セキュリティに強い担当者に任せれば解決するわけでもない。基準に沿って、汎用的なセキュリティ対策を勘案し、システムの特性や構成を踏まえて、組織的に対応しなければならない。

アマゾン ウェブ サービス（AWS）では、エンタープライズ領域での様々な問題解決や、より早くシステムを構築するために、各種サービスが提供されている。これらのサービスは日々改善されており、かつ、新しい有益なサービスも提供されている。しかしながら、多種多様なサービスが存在するため、関連するセキュリティ情報を探すだけで大きな手間がかかる。

2 目的

このように、クラウド活用におけるセキュリティやコンプライアンス対応への重要性が増している。適切なセキュリティの獲得は、技術面（情報漏洩や攻撃防御など）のみ対策を講じてもたどり着けない。コストリスクやサービス終了リスク、法的リスク、災害リスクなど、様々なリスクに対しての対処方法を考慮し、どのようにシステムを構想していくかが求められる。このため、設計や実装例の技術的な項目のみならず、クラウド導入に向けての企画や調達工程でのリスクへのアプローチも必要であると本コンソーシアムでは認識している。

このため、クラウドを利用する企業において、クラウド活用の適切なリスク管理のあり方を考慮し、安心と安全の確保に向けて、組織的な継続性を持てるセキュリティシステムの新たな姿の検討を目的に、本ガイドラインの整備に着手した。

3 構成

本ガイドラインでは、各リスクに対して管理策をマッピングし、優先度の高いリスクに対応できる設計になっているかの評価を可能にする。さらに、様々な管理策に対応する AWS サービスやその機能の紹介、具体的な設計・実装例を紹介している。本ガイドラインは、クラウドおよびクラウドセキュリティに関わる 7 つのテーマで構成している。

- トレンド（4.1）
  過去からの経緯も含めて、クラウド導入のトレンドや、クラウドを取り巻く環境を紹介

- クラウドジャーニーと AWS Cloud Adoption Framework（4.2）
  組織がクラウドを導入するための設計とプロセスをサポートするクラウドジャーニーと AWS Cloud Adoption Framework をベースに「クラウドを活用してビジネスを成功させる道のり」を紹介

- 責任共有モデル（4.3）
  セキュリティとコンプライアンスはクラウド事業者と利用者との間で共有される責任であることを認識し、クラウドの利活用における役割分担の定義を説明。また、クラウドの実運用経験から、様々なステークホルダー間での責任分解点の考え方を紹介

- クラウド導入に適応したリスクコントロール（4.4）
  Cloud Risk Control Framework（リスクアプローチによるクラウド利用の評価フレームワーク）から、公知のガイドラインとのマッピングによる最適化されたリスクコントロールマトリックスを説明し、リスクへの取り組み方を紹介

- 構築時におけるリスクへの対策（4.5）
  Cloud Risk Control Framework での技術的エリア「C4.クラウドサービス利用における継続的構築・運用」におけるリスクの具体例と対策を紹介

- AWS サービス（4.6）
  AWS は、安全かつ高パフォーマンス、障害耐性を備えた効率的なアプリケーション用インフラストラクチャを提供している。セキュリティ要件を満たすために必要となる、セキュリティ関連のサービスを紹介

- 設計例（5）
  実際に構築されるシステムの構成を踏まえて、具体的なリファレンスアーキテクチャ図をベースに、AWS サービスを利用したセキュリティ対策の設計方針を示す。

3.1 対象読者

あらゆる企業でクラウドのメリットを享受するために、ガイドラインを活用し、セキュリティ的な対策を講じることが、本コンソーシアムの目的の一つである。諸外国と比較した場合、日本におけるシステム構築では、SIer 企業への依存度が大きいため、クラウドの導入を支援する SIer 企業の現場エンジニアからマネジメントがガイドラインの主な読者と位置づけている。

初めてクラウドを導入するエンジニアには包括的な対策方法を理解いただく。既にクラウドを利用しているエンジニアには、知識を向上し、構築プロセスの改善を実現していただく。マネジメントの方には、セキュリティリスクやコストの増加を懸念される、支援先のユーザー企業への説明責任を果たすためにガイドラインが活用できる。

SIer 企業のみならず、クラウドを利用し、事業やサービスを運営するユーザー企業においても、エンジニアであれば、ガイドラインを活用し、構築するシステムのセキュリティ的な妥当性を検証できる。マネジメント層では、業務とサービス優位性を勝ち取るために積極的なセキュリティ対策が有用なことを理解していただく。

役割に関わらず、本書のすべてを参照していただきたいが、最初に読むのが望ましいパートは役割毎に以下の参照をお勧めしている。

SIer 企業：エンジニア 実際の AWS の設計や構築にてセキュリティ対策を施す （「4.6.AWS サービス」から参照）	ユーザー企業：エンジニア 構成に対してどのようなセキュリティ対策が必要かを考える （「4.5.構築時におけるリスクへの対策」から参照）
SIer 企業：マネジメント クライアントへクラウドでのセキュリティを説明する （「4.3.責任共有モデル」から参照）	ユーザー企業：マネジメント クラウドにおけるセキュリティを理解する （「4.1.トレンド」から参照）

図 1：対象読者と利用ガイド

4 セキュリティを高めるために考えるべきこと

4.1 トレンド

4.1.1 クラウド全体のトレンド

1990 年代にインターネットの急速な普及により、様々な用途でコンピュータが利用され、主に通信事業者にて、ホスティングやコロケーションサービスが隆盛した。また、アプリケーション機能をネットワーク経由で提供する ASP サービスも、この時期に普及し始めた。しかしながら、当時は高速なネットワーク環境がなく、各企業の業務に合わせたカスタマイズもできない状況から、ASP は限定的な利用に留まっていた。

2000 年代のブロードバンド普及により、従来の ASP の課題を解消したサービスが SaaS（Software as a Service）として普及し始めた。またクラウドコンピューティングという言葉が認知され始め、PaaS（Platform as a Service）や IaaS（Infrastructure as a Service）という様々な形態でのクラウドコンピューティングサービスが開始された。このように、2000 年代に、コンピュータを「所有する時代」から「共有する時代」への変化が始まった。

しかし、クラウドサービスの利用において、新たな課題やリスクも顕在化してきた。アカウント侵害の規模拡大や、API への自動化ボットによる攻撃、利用者側による設定ミスなどクラウド特有のリスクがある。かつ、それをマネジメントするにも、クラウドの特性を理解した上でのコンプライアンスやガバナンスを整備しないといけない。

また、現在のコロナ禍においては、リモートワークが前提となり、社内資料の管理、従業員や顧客の情報管理などをクラウドへ移行し、社外からのアクセスを可能としている。加えて、モビリティや個人の生産性、シー

ムレスな BYOD の提供といった要求に応えるため、社外からの機密情報へのアクセスは増大している。クラウド上での情報管理の徹底と、外部からの想定できない攻撃から守るための対策は、どの企業にも関わる最優先の課題である。

このように、従来のオンプレ環境とは異なり、クラウド環境には特有のリスクがあるため、そのリスクを識別し、適切なセキュリティ対策が求められる。企業が取るべき対策は、使用ルールの明確化、モニタリングの強化、従業員教育に加え、クラウドセキュリティサービスの導入が挙げられる。

クラウドサービス上で構築したシステムの可用性やセキュリティは、最終的にサービス利用者が担保しなければならない。それには利用するクラウドサービスに対する深い知識やスキルが必要となる。一方で、肝心のクラウドサービスに関連するスキルの取得は現場任せなのが散見されており、組織的な取り組みができていないという課題がある。

4.1.2 AWS でのトレンド

AWS は、2000 年代初頭に Amazon Elastic Compute Cloud（Amazon EC2）、Amazon Simple Storage Service（Amazon S3）のサービスから始まった。現在では様々なタイプのデータベース、セキュリティ、ビッグデータ＆機械学習、IoT 基盤などの 175 を超えるサービスがリリースされており、加速しているデジタルトランスフォーメーション化に求められる多くの機能を有している。これらのサービスは世界 190 の国・地域で利用されており、パブリッククラウドの世界的シェアは約 5 割である（注 10）。サービスは、全世界に分散している設備で提供されており、設備は 24 のリージョン、77 のアベイラビリティゾーン、210 超のエッジロケーションまで拡張している。ユーザー数に至っては全世界で数百万（日本国内十万以上）に達している。様々なビジネスシーンでの利用以外に、4,000 超の公共機関、9,000 超の教育機関でも利用されている。

このように、利用者の規模から、AWS はきわめて重要な社会インフラとして位置づけられる。したがって、セキュリティ面の万全な対策は、可用性や耐障害性と同等以上に重要性があると AWS では考えられている。

AWS では、多種多様な形態のシステム運用をサポートする、様々なセキュリティサービスを提供している。サービス利用開始時から強固なアクセスコントロールと、証跡の取得が可能であり、現在に至るまで、毎年セキュリティ系のサービスや機能が追加されており、システム運用のセキュリティ品質強化に寄与している。

表 1 AWS でのセキュリティ関連のサービスリリース時期

年	リリースされたサービス
2009	Amazon Virtual Private Cloud（アクセスコントロール）
2011	AWS Identity and Access Management（アクセスコントロール）
2013	AWS CloudHSM（暗号化）、AWS CloudTrail（ロギング）
2014	Amazon Cognito（アクセスコントロール）、AWS Key Management Service（暗号化）、AWS Directory Service（アクセスコントロール）
2015	AWS WAF（攻撃防御）、AWS Shield（攻撃防御）
2016	Amazon Inspector（検知）、AWS Certificate Manager（暗号化）、AWS Artifact（リファレンス）
2017	Amazon GuardDuty（検知）、Amazon Macie（検知）、AWS Single Sign-On（アクセスコントロール）
2018	AWS Secrets Manager（鍵管理）、AWS Firewall Manager（攻撃防御）、AWS Resource Access Manager（リソース共有）
2019	AWS Security Hub（状況確認）
2020	Amazon Detective（調査）

経年でセキュリティ関連のサービスが洗練され、利便性が向上する一方で、以下のように、新たな課題が生じてきた。

- データベースやビジネスアプリケーション、コンテナなどのサービス拡充によるセキュリティ管理／運用における手順の複雑化
- 利用サービス増加によるセキュリティアラートの増加
- アカウントや各サービスの複雑化による、セキュリティ状態チェックの手間増加

このように、複雑化するセキュリティ対策での運用作業に対して、2019 年に登場した「AWS Security Hub」が解決策を提供した。AWS Security Hub では、複数アカウントで利用している様々なセキュリティサービスのデータを集約し、一元的な可視化が可能である。更に、可視化のみではなく、CloudwatchEvents 経由で Lambda と連携し、対応したいアクションの自動化または、Detactive との連携による調査を容易に可能とした。このサービスにより、エンタープライズにおけるセキュリティ対策での運用作業の画期的な改善が望める。

しかしながら、新しい取り組みの採用は、現行作業の変化による学習コストや、オペレーションミスによる障害も懸念される。また、そもそも追加されるサービスの内容を知らなければ、たとえサービス自体が有用な仕組みを持っていたとしてもシステムへ適用されず、メリットが享受できない。スキルの取得にも課題はあるが、リリースされるサービスを認知し理解する活動も組織に求められる。

4.2 クラウドジャーニーと AWS Cloud Adoption Framework

4.2.1 クラウドジャーニー

一方、クラウドの採用に踏み切る場合に、セキュリティ対策も含めて、「何をどこまでやれば良いのかが、まったくわからない。本当に大丈夫なのかどうかも不明」という状況もある。問題点が明確であれば、打ち手を講じられるが、そもそも、どこまでを考慮すれば良いのかが曖昧であり、使い始めてから問題に気づく場合も多々ある。また、クラウド化の対象が単一システムであれば、影響範囲は小さくもあるが、エンタープライズなシステムでは、連携するシステムも多いため、影響範囲調査だけでも相当のコストがかかる。しかしながら、今後の更なるクラウド化が待ったなしで迫ってくるため、即座に全社的な取り組みを強いられる可能性が高い。

企業におけるクラウド化への取り組みは一過性のものではなく、継続的な取り組みであり、クラウド化対象と定義する情報資産の全クラウド化により完結する。この継続的な取り組みを「旅路」(ジャーニー)に例えて、クラウドジャーニーという言葉が誕生した。クラウドを活用してビジネスを成功させるための道のりをクラウドジャーニーとし、4 つのステージで区別される。

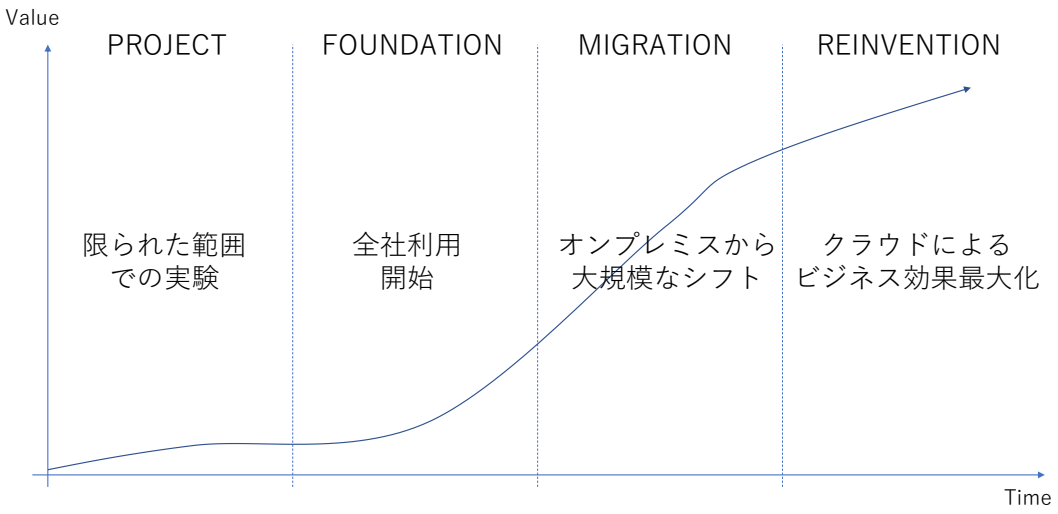


図 2:クラウドジャーニーにおける 4 つのステージ

Stage1:Project

最初は、いくつかのプロジェクトにてクラウドを利用し、ビジネスニーズを満たす方法を理解する。多くは、既存システムをクラウドにそのまま載せ替えるリフト形式を採用しがちである。十分に学習した技術者が存在する場合には、クラウドネイティブな仕組みを考えて、クラウド化へ取り組むかもしれない。いずれにせよ、ミッションクリティカルなシステムからクラウド化に取り組むというよりは、影響の少ないシステムを対象にし、数回の実験的なプラクティスを得ていく。このステージにおけるテーマには以下がある。

- 特定条件のために利用
- 効率的な選択肢かどうかの検証
- 限られた人が多くの経験を積む
- 社内での有識者認知

Stage2:Foundation

実験的な取り組みからのナレッジ活用や、有識者集団がそろった組織の立ち上げ、本格的な全社展開へ取り組むステージ。取り組みが拡大していくため、セキュリティへの対応、設計品質の維持、情報共有、スキル習得など、システムのクラウド化と同時に取り組むべきタスクが増加していく。これらのタスクへの取り組み次第で、将来のクラウド化の効果が左右される重要なステージ。このステージにおけるテーマには以下がある。

- 基礎を固めながら小さな成功を積み重ねる
- 推進組織が立ち上がる
- ガイドラインや環境の整備
- 徐々に本番稼働
- 既存データセンターと接続

Stage3:Migration

新システムの構築はクラウドありきで考え、既存システムは段階的にクラウドへシフトしていくステージ。クラウド基盤が構築されており、多くのプロジェクトで経験を積んでおり、組織がどう取り組むべきかがシステマチックに対応できる状態である。このステージにおけるテーマには以下がある。

- 全社的に利用しビジネス効果を享受
- IT 戦略におけるクラウドの位置づけが明確になる
- 多くのシステムが移行
- 推進組織が確立
- 十分な実績やナレッジが蓄積される
- データセンターの縮小

Stage4:Reinvention

クラウドを軸に最適な組織にシフトしており、サービスや業務でのクラウドの最適な利用と、クラウドでのシステム運用の最適化と自動化を成しえているという完全に成熟した状態。このステージにおけるテーマには以下がある。

- クラウドを最大活用しビジネスを最大化
- クラウドがデフォルトの選択肢となる
- 「なぜクラウドなのか」から「なぜクラウドではないのか？」に変わる
- アーキテクチャ、運用、組織が最適化

最初の Stage1 では実験や学習の機会を含むため、手探りで進むこともあるが、Stage2、3 での取り組みが直感的であったり、根拠なく進めているようでは、設計の誤り、手戻りによるコスト増、時間の喪失が発生する可能性が高い。「クラウド化は失敗した」と判断されると、次のステージへ遷移できず、中途半端な状態となり、更なるコスト高やセキュリティリスクが発生しがちである。そもそも、ビジネスモデルや業務プロセスをクラウドのメリットを得られる状態に移行することが目的であり、何も技術的なクラウドの導入が目的ではない。この目的を踏まえて、クラウドを最大限に活用した、自社の求めるシステムの実現には、全社組織で考えた綿密な計画と適切なアプローチが必須である。

4.2.2 AWS Cloud Adoption Framework の活用

AWS は、クラウドを導入するための設計とプロセスのサポートを目的とした AWS Cloud Adoption Framework（AWS CAF：クラウド導入フレームワーク）（注 11）を提供している。フレームワークで示されているガイダンスは、IT ライフサイクル全体で、組織全体にわたるクラウドコンピューティングへの包括的なアプローチの構築に役立てられる。AWS CAF は、関連するステークホルダーの観点から、パースペクティブと呼ばれる 6 つの重点分野で編成している。Business、People、Governance のパースペクティブではビジネス遂行能力に焦点を当てており、Platform、Security、Operations のパースペクティブでは技術的能力に焦点を当てている。

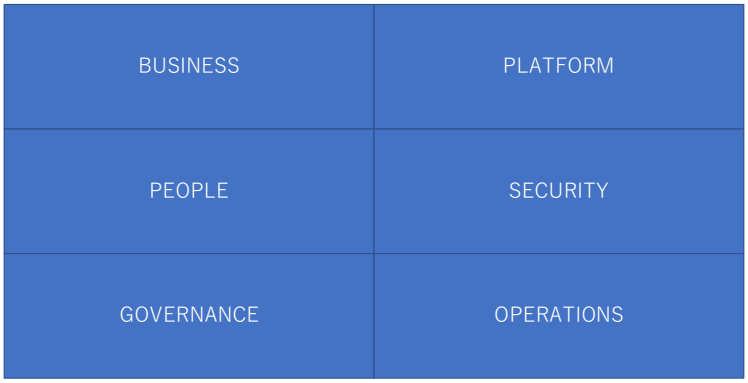


図 3：AWS CAF での 6 つの重点分野

それぞれのパースペクティブでは、責務とステークホルダー例、求めるケイパビリティ（クラウド導入により変革するスキルとプロセス）を定義しており、検討すべき項目を示している。

ジャーニーのステージに合わせて、これら 6 つのパースペクティブのそれぞれの責務を意識し、ステークホルダーを適切に関与させ、プロセスとスキルを発揮していただくように、計画する。計画では、組織の現在の状態、目標とする状態、および目標とする状態に到達できるかの分析が必要であり。各パースペクティブへリソースを配置し、プロセスの実行とスキルが充足できるかをマッピングし、計画の実現性を検証していく。

4.2.3 Cloud Discovery Workshop による AWS CAF へのマッピングからロードマップ策定

AWS CAF のパースペクティブ分析を一人で検討しても、思うように進まない。企業における今後の方向性の決定であり、そもそも一人で決めきれるはずがない。

様々な決定権を持つステークホルダーを参集させ、AWS CAF の観点で意見を持ちより、協同での現状整理が必要である。AWS では、Cloud Discovery Workshop（CDW）のワークショップ形式を採用し、1 日ほどの短期集中で、状況の可視化と議論、共有による AWS CAF の整理を紹介している。CAF の観点で現状の課題を整理し、優先度を確認した上で、クラウド導入ロードマップを作成する。CDW は「ゴール像の確認」「課題の洗い出し」「課題の分類」「課題の優先順位付け」「対策の議論」「ロードマップ作成」のステップで実行される。

CDW の開催により、組織全体にわたるクラウドコンピューティングへの包括的なアプローチが構築できる。AWS CAF のパースペクティブを用いて、各組織の役割分担や課題および対策が明確になり、ロードマップとして具体的な今後の計画が明らかにできる。

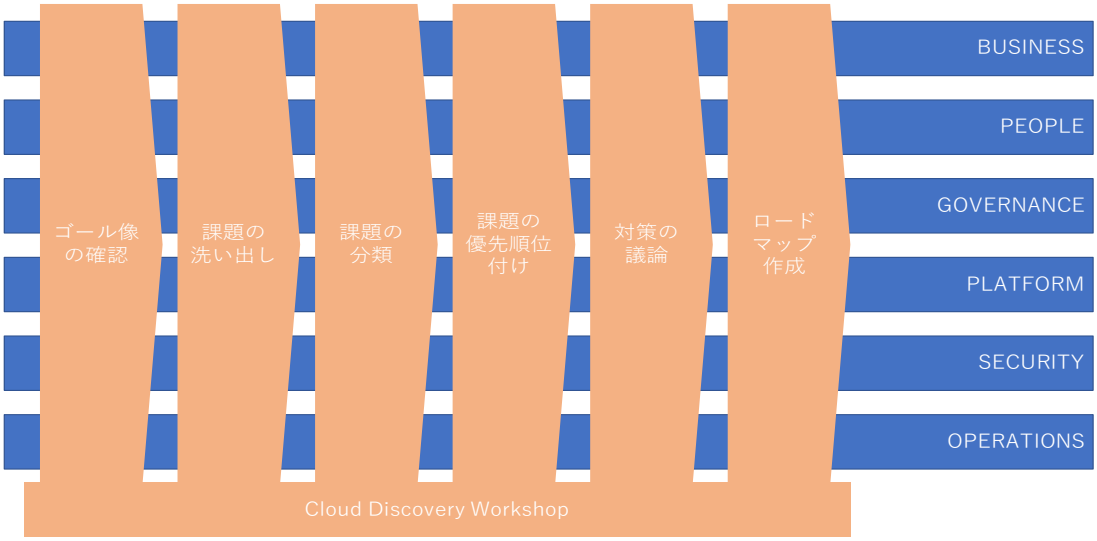


図 4：Cloud Discovery Workshop での検討プロセス

ワークショップの参加者には、自社内のリソースだけでなく、クラウド化の取り組みに十分な知見を持った社外の有識者の参加を検討いただきたい。自社リソースのみで検討しても、ゴールの網羅性がなかったり、課題の洗い出しにて、重要な課題が欠落する場合がある。また、自社の状況を理解している強みはあるが、前提知識に縛られて、ボトムアップ的な小さなゴールと効果の薄い解決策の打ち出しに始終する場合がある。社外の有識者を活用し、他社事例による自社との比較やトップダウンでゴールと課題を考えての意見交換をお勧めする。

4.3 責任共有モデル

4.3.1 モデルの定義

セキュリティとコンプライアンスは AWS と利用者の間で共有される責任である。下図の責任共有モデルでは、"ホスト"オペレーティングシステムと仮想化レイヤーから、サービスが運用されている施設の物理的なセキュリティに至るまでの要素を AWS が運用、管理、および制御する。利用者（下図、利用者部分）は、”ゲスト”オペレーティングシステム（更新とセキュリティパッチを含む）、その他の関連アプリケーションソフトウェア、および AWS が提供するセキュリティグループファイアウォールの設定に対する責任と管理を担う。

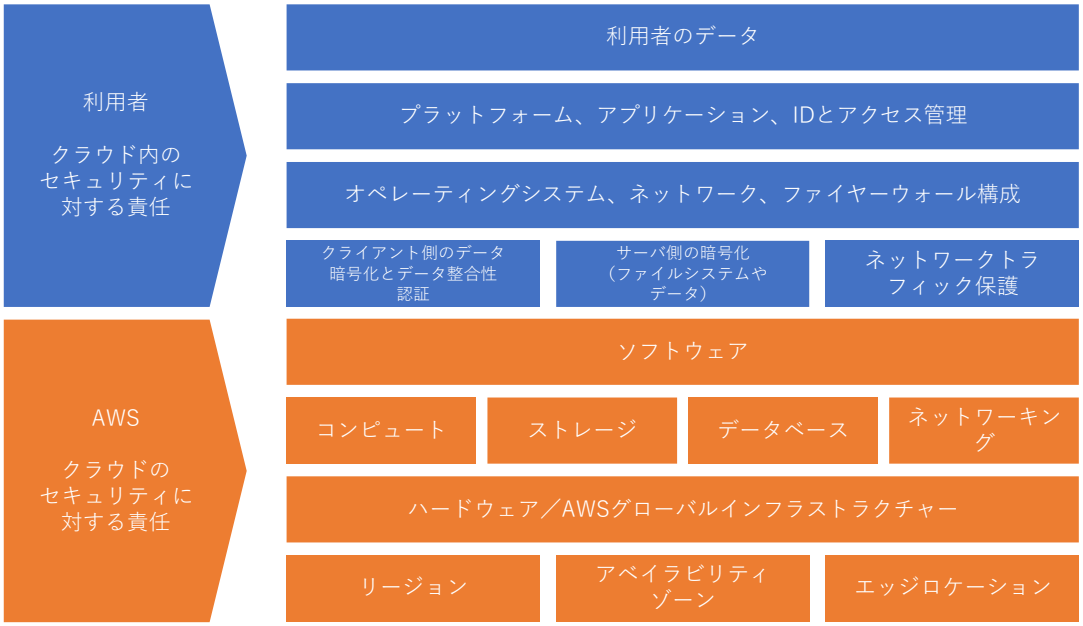


図 5: 責任と管理の分担による責任共有モデル

https://aws.amazon.com/jp/compliance/shared-responsibility-model/から引用

この責任共有モデルは AWS の利用前に最初に理解しておくべき事項である。AWS の利用の前に、利用者は AWS の責任共有モデル（※x フッターに URL 記載で）のページへアクセスし、内容を理解しなければならない。

AWS と利用者との責任への位置づけは、Security “of” the Cloud（クラウド“の”セキュリティ）と Security “in” the Cloud（クラウド“における”セキュリティ）とに区別されている。

Security “of” the Cloud は AWS 側の責任範囲であり、クラウドで提供されるサービスすべてを実行するインフラストラクチャの保護に責任を負う。AWS が自身の担当する範囲に対して、どのようにセキュリティへ取り組んでいるかの『正しい認識』が利用者には求められる。Security “in” the Cloud は利用者側の責任範囲であり、クラウド内のセキュリティに対する責任である。利用者の責任範囲は、利用者が選択する AWS

のサービスによって異なる。選択したサービスの特性を理解し、セキュリティを鑑みた『適切な使用』が利用者に求められる。

4.3.2 『正しい認識』のために AWS の公開情報へアクセス

セキュリティは、AWS での最優先事項と位置付けられている。AWS から、担当する責任範囲への取り組みを証明するための情報が公開されている。安全で規制に準拠したクラウド環境を運用できるように、様々な要件に合わせられる、各種コンプライアンス報告書、証明書、認定書も用意されている。
※AWS を利用している場合、AWS Artifact というサービスを利用して、証明書、認定書、監査レポートをダウンロードすることが可能

AWS による情報の公開は「公開情報」、「ホワイトペーパー」、「第三者認証」の 3 つ提供形態がある。利用者は『正しい認識』のために、これらの情報へアクセスし、内容の理解をお勧めする。

表 2 AWS でのセキュリティに対する取り組みへのアクセスリスト

公開情報	データセンター https://aws.amazon.com/jp/compliance/data-center/data-centers/ 「境界防御レイヤー」として、データセンターの物理的なセキュリティ対策の説明。「インフラストラクチャ・レイヤー」として、データセンターの建屋、各種機械、およびそれらの運用に係るシステムの説明。「環境レイヤー」として、データセンターの立地選択、建設、運用・維持に至るまで、環境に固有の要因についての説明。「データレイヤー」として、カスタマーデータエリアへの防御策の説明
	コントロール https://aws.amazon.com/jp/compliance/data-center/controls/ 「セキュアな設計」、「ビジネスの継続性と災害復旧」、「物理アクセス」、「モニタリングとログ記録」、「監視と検出」、「デバイスの管理」、「運用サポートシステム」、「インフラストラクチャのメンテナンス」、「ガバナンスとリスク」への取り組みを説明
	データプライバシー https://aws.amazon.com/jp/compliance/data-privacy-faq/ プライバシーとデータセキュリティのために適用しているポリシー、実施策、テクノロジーを説明
ホワイトペーパー	コンプライアンスのリソース https://aws.amazon.com/jp/compliance/resources/ 「AWS コンプライアンスクイックリファレンスガイド（2018 年 5 月）」や「AWS リスクとコンプライアンス概要（2017 年 1 月）」、「主要なコンプライアンスに関する質問と AWS の回答（2017 年 1 月）」、「AWS セキュリティのベストプラクティス（2016 年 8 月）」などのホワイトペーパー
第三者認証	AWS コンプライアンスプログラム https://aws.amazon.com/jp/compliance/programs/ AWS が順守する CSA、ISO、SOC,PCI DSS などの認証情報の提供
	コンプライアンスプログラムによる AWS 対象範囲内のサービス https://aws.amazon.com/jp/compliance/services-in-scope/ 各認証要件にそれぞれのサービスが対応しているかの情報提供

次に、個別のサービスがどのような機能を有しているかを理解するが、本ガイドラインでは、個別サービスの詳細な機能説明は割愛とする。AWS のサイトに、提供しているサービスそれぞれのガイドやチュートリアル、テクニカルリファレンス、導入事例があるので、そちらを参照いただきたい。(注 12)

セキュリティの側面で、利用者が考えるべき観点は、提供される機能それ自体の優劣ではなく、システム内でのデータの所有と管理の責務であり。このため、以下の 4 つを常に意識して、設計と実装を検討する。

- セキュリティリスクがないか？
- どこにデータを保存するか？
- アクセス権を誰に付与するか？
- 適用される法令があるか？その順守には何が必要か？

クラウドサービスでは、SaaS、PaaS にて定義されるように利用形態に違いはあるにせよ、セキュリティのすべてをクラウド事業者へ押しつけることはできない。リスクの移転を考えるのではなく、リスクへの対策を、役割分担して、協同で対応していく。責任の所在を曖昧にせず、各々の責務をもって担当するため、AWS の「責任共有モデル」のように、役割分担の境界の認識が重要である。利用者側がセキュリティを意識し、担当する領分に関するリテラシをあげ、責任をもって適切に対応していく心構えが必要である。

4.3.3 運用時でのモデル実現における課題

AWS と利用者側とで責任共有モデルをリファレンスとし、それぞれの責務を遂行するが、実際の運用では、利用者側に各種課題が発生する。これらの課題の存在を事前に認識し、組織的な取り組みと計画性をもっての運用が求められる。

利用者内に、さらなる”責任共有モデル”がある

責任共有モデルは、AWS と利用者の二階層にわかれている。しかし、現実では、利用者内に多層の役割分担が存在する。日本の事業会社の多くは、SIer へシステム開発を依頼するが、アプリケーション開発は A 社と B 社、アプリケーション保守は C 社、インフラ運用とアプリケーション監視は D 社というように、工程と役割をわけて数社が対応するケースがある。また、事業会社の中でも、システム部門や業務部門、監査部門など、各署がシステムに関係する。セキュリティへの責任を関係者間で共有し、どのように協働していくかの協議と明文化が重要である。

解決手段への自縛

例えば、PCI DSS(注 13)を取得する場合、全ての要件への対応を自社でまかなうには非常に大きなコストがかかる。AWS は PCI DSS を含めた様々なコンプライアンスプログラムに対応しており、AWS の活用により、利用者が認証への対応範囲の縮小が可能である。一方で、完全なるセキュリティコントロールに固執

し、マネージドサービスを利用せず、オンプレ同等の仕組みを、そのままクラウド化しただけでは、セキュリティに関連する負荷は低減できない。あるべき論とセキュリティ対策での経済性を考えて、組織がガバナンスとして何を重要とするかの考えに基づき、役割分担として、AWS を信頼した選択をすべきである。また、個別サービスにおける技術的な解決も、責任分担として利用者側が対応するが、解決策の完全なる導出までもが利用者へ求められてはいない。AWS では、サポートや、技術支援、コンサルティングサービス、トレーニングサービスなど、様々な形での組織的な支援がある。悩み過ぎずに AWS へ相談し、解決策へつながる理解を深めるのも利用者側の責務の一つでもある。

ライフサイクルへの対応

オンプレミスのシステムでは 10 年以上構成を変更せずに利用しているものもある。一方、クラウドでは、サービスのサポートや提供は時限的であり、将来、サービスが停止する可能性がある。このため、オンプレミスでの運用のように環境を塩漬けにし、システムを使い続けることはできず、サポートする OS の期限切れや、インスタンスタイプの廃止は将来確実に発生する。利用者は、いつにどのようなサービスが利用できなくなるかのリスクを把握し、システムを最新化していく計画を検討しなければならない。

利用者に主体的なコストガバナンスが求められる

クラウドのメリットの一つは従量課金だが、各種サービス利用の時間と量をコントロールしないと、予算枠を超過する場合がある。本番環境以外に、テスト環境や開発環境も含め、利用料のしきい値を適切に設定し、アラートを発報するサービスを用いて、上限超過を未然に防ぐ取り組みが必要である。また、利用料の実績値から将来を予測し、固定費用で組んでいる IT 予算計画が変動するものとして考えなければならない。このように、クラウドの利用においては、利用者側での主体的なコストガバナンスが求められる。

多数の AWS アカウントの管理

多数のシステムで AWS を利用する場合、システム毎に、AWS アカウントを作成する場合がある。加えて、ステージング環境やテスト環境、開発環境での管理アカウントも分けての作成する場合もある。このような環境に対して、アカウントを横断したコストや運用の一元化を目指すが、アクセス管理や利用部門へのコスト配賦も考慮してのアカウント管理を最初に設計しなければ、後からの変更に手間がかかり、管理作業に手間をとられる場合がある。

4.4 クラウド導入に適応したリスクコントロール

クラウドの利用では、従来のオンプレ環境とは異なったセキュリティ対策が求められる。採用するクラウドのサービス特性を理解し、暗号化や脆弱性対策、アクセス管理などの技術面に加え、利用ポリシー策定や人材育成、法令順守確認などの戦略や管理態勢等の総合的な対策が必要とされる。しかしながら、発散的に思いつく限りの対策を洗い出し、それぞれ対応しても、包括的に有効な状態を達成できるかどうかが判断できない。

この課題を解決するために、クラウド利用における戦略・管理態勢および技術等に対するアプローチを体系的にまとめた、本コンソーシアム独自のフレームワーク「Cloud Risk Control Framework」（CRCF）がある。CRCF は、ビジネスでのクラウド活用において、ビジネス発案後、どのようにクラウドを含むシステム選択を実施していくか、またクラウドを効果的に利用する場合にどのような観点でアプローチを実施する必要があるかの体系的な整理を目的として作成した。CRCF では、クラウド利用の準備と選択検討、選定、構築という、4 つのセクションに分けており、セクション毎にとるべき管理策を定義している。

C1. システム化検討・要件整理

新たなビジネスプランを策定した際に、組織の IT 戦略との整合性や IT システムに求める要件、IT 導入に向けて必要となる体制・人材のリソース等、システム化を効果的かつ漏れなく実施するために、まず整理すべき事項を定義する。IT システム化を実施する際に、対象業務のみへの着目では、個別最適は実施されるものの、組織としての全体最適となっていない状況がある。また、IT システムに求める要件が不明確な場合、システムが業務要件を満たしているか、十分に判断できない事象ある。これらのことから、システム化を検討するうえで必要となる項目を整理している。

C2. 基本システムの検討

IT システムに求める要件の整理後、そのシステムをどうやって実現するかを検討し、選択する必要がある。対象システムの前提となる環境（企業の IT 環境との関連性、接続先システム等）を考慮したうえで、ベースとなるシステムデザインを検討する。その検討の 1 つに、クラウド利用の選択が含まれている。クラウド利用を選択した場合は、各種クラウド事業者が提供するサービスからビジネスに合致するサービスを選択する必要があるが、デザインレベルの検討では、サービスが結果的に合致しないことやサービス終了の可能性も考慮し、代替策も含めた検討も必要となる。また、IT システム投資として見合ったものになるか、初期コストや運用コストも試算しておく必要がある。

C3.クラウドサービス事業者の選定

IT システム環境にクラウド利用を選択した場合、責任分界点を意識したシステム構築・運用が必要となる。責任分界点において、クラウド事業者側の責任範囲となっている部分は、クラウド利用者側からコントロールができないため、クラウドを選択する前に、対象のクラウド事業者で問題ないかを判断する必要がある。また、クラウド利用者側の責任範囲の領域でも、クラウド事業者から提供される機能を利用しなければ実装

できない状況が発生する。そのため、実現したい構成やセキュリティ対策を実装するための機能を、クラウド事業者が漏れなく提供しているかを確認する必要がある。これらのクラウドに求める機能を満たせられるクラウド事業者を選定するための項目を、当セクションでは整理している。

C4.クラウドサービス利用における継続的構築・運用

クラウド利用したうえで、各システム構築・運用に必要となる項目を整理している。本書において、CRCF の中でクラウド利用時における一般的な各種管理策は「4.5. 構築時におけるリスクへの対策」に記載している。AWS の構築での必要となる具体的な対応策は設計例として「5.設計例」に記載している。

4.5 構築時におけるリスクへの対策

本ガイドラインでは、CRCF の C4 での「クラウドサービス利用における継続的構築・運用」をターゲットに、実行すべきセキュリティ管理策を示す。C4 での管理策は 15 個ある。この 15 個のそれぞれで、クラウドを利用する場合での各種セキュリティへの取り組みとして利用者側が実施していく対策を紹介する。また、管理策が欠落する場合に直面するリスクと、そのリスクが具体的にどのようなものかも説明している。

C4-1：クラウド構築検討

エンタープライズにおけるシステムの開発は一過性ではなく継続的であり、かつ個別システムのみの対応でなく全社的に統一された組織だった取り組みが求められる。クラウドを活用したシステム構築では、システム要件に適合する各種クラウドサービスを利用するが、クラウド化の要求に任せて、対症療法的にシステムを構築していては、セキュリティガバナンスが取りづらい。このため、対象範囲と将来を踏まえて、どのようにクラウド環境を構築していくかの方針定義や計画策定、クラウドサービス利用の全社ガイドラインの策定が求められる。方針および計画には、障害を想定した可用性の検討も含まれる。また、システムのサービス提供自体に関わるクラウドサービスの取り扱い以外に、リリース方式や、構成管理、運用からのフィードバックの取り組みなど、運用側面から取り上げられる課題の解決を、次の構築へつなげる取り組みも求められる。これら、一連の手続きに関しては、効率化やセキュリティ対策を目的とした、自動化の導入も考慮事項に含まれる。

C4-2：クラウド運用検討

システム運用に関わる様々な定常/非定常の作業をトップダウンで洗い出し、運用作業の全体を定義する。作業には、定型/非定型での対応があり、文書化できる範囲を考えて、各作業の設計と手続きを明らかにする。運用作業は PDCA サイクルに基づき、永続的に改善が求められる作業である。設計と手続きの内容が妥当かを検証するために、運用実施前と実行時におけるレビューを計画しておく。実際の作業においては、作業改善へのインプットとなるように、作業品質のクライテリア定義と測定方法を検討しておく。クライテリアを満たさなかった作業では、運用手順を見直す。クラウドの利用においては、運用効率や運用品質の向上

が見込める新しいサービスが都度リリースされている実績がある。このような、より価値のあるサービスへの乗り換えに伴っての運用手順の見直しも求められる。これら、一連の手続きに関しては、システム構築検討と同様に、効率化やセキュリティ対策を目的とした、自動化の導入も考慮事項に含まれる。

C4-3：サービスリソースに係る運用作業

サービスリソースに影響する業務・運用イベントを整理し、必要に応じて臨時のリソース増強の手続きを定める。また、利用するクラウドサービスに関して、サービスクォータを確認し、必要に応じて設定されているクォータの引き上げが可能かをクラウド事業者へ確認しておく。短期的なイベントへの対応以外にも中長期的な取り組みとして、キャパシティプランニングを策定し、利用しているサービスのリソース増強を計画する。精緻な計画のために、各サービスのリソース状況のモニタリングから、キャパシティを試算するパラメータをハンドリングする仕組みを設計する。また、増強の手順が困難でないかや、変更によるリスク（サービス停止やリソースを戻せないなど）がないかも確認しておく。

C4-4：システム監視

システムの安定運用のために、クラウドサービスと運用するシステムからの発報をハンドリングする。クラウドのサービスから発報されるイベントは非常に多いため、監視対象とするべきイベントかどうかの判断がつきにくい。このため、運用開始前に、各サービスでのイベントマニュアルを確認し、どのような発報をハンドリング対象とするかを設計する。設計後、発報の集約をどのようなサービスを利用して、適切な担当者へ通知するかの手続きを検討する。また、クラウドサービス以外にも、作成したアプリケーションやインストールしたミドルウェアのログ情報内の監視対象とする情報もハンドリング対象とし、クラウドのサービスでの発報と合わせて一元管理できる仕組みを設計する。加えて、サービスポータル等を通じてクラウドサービス自体の稼働状況についても、継続的に情報を収集する。

C4-5：コスト管理

クラウド利用は従量課金となるため、クラウド利用方法やシステム構成によって、コストが大きく変動する可能性がある。そのため、事前の試算をもとにして、定期的にコスト管理を実施する。月次ベースでの予算設定と閾値を設定し、日次の累積コストから、予算を超過しないかを自動的にモニタリングする。あわせて、これまでのコスト実績を定期的に棚卸しし、今後のコスト予測により、必要に応じて構成の見直しを実施する。加えて、不要なコスト利用を防ぐため、リソース使用率を監視し、枯渇または余剰なリソースに対して、定期的なスケールアップ/ダウンを実施する計画を策定する。また、各業務の売り上げと、それに紐づく各種コストを投資対効果として確認する必要がある場合、部門内でのクラウド費用負担へ対応できるように、適切なアカウント管理も鑑みてコスト管理を検討する。

C4-6：新規サービスの検討

クラウドサービスには、様々なサービスがあり、日々、サービスの改善と新しいサービスがリリースされている。しかしながら、そもそも追加されるサービスの内容を知らなければ、たとえサービス自体が有用な仕組みを持っていたとしてもシステムへ適用されず、メリットを享受できない。このため、リリースされるサービスを認知し理解する活動が組織に求められる。また、新しいサービスの適用においては、拙速に適用とせず、影響範囲の特定と検証が必要である。このような適用に向けての手続きを明らかにし、実施においては、計画を策定しての取り組みが求められる。また、新サービス採用につながるような、利用しているサービスのサービス提供停止にも合わせて注意しなければならない。注意するには、クラウド事業者から事前に提供される、サービス停止に関わる情報をチェックする必要があるが、この場合においても、新サービスの適用と同等に影響範囲の特定などの対応が求められる。

C4-7：マルウェア対策

クラウドサービスの利用において、システムを稼働させるオペレーティングシステムの運用責任は利用者側にある。このため、オペレーティングシステム上でのマルウェア対策は利用者側で対応する。クラウド事業者側でマルウェア対策が取れるサービスにどのようなものがあるかの確認から始まり、対策ツールの導入計画と、実施手順を明らかにする。AWS で考えると、対策ツール自体を提供していないため、利用者が独自に最適なツールを取り入れ、クラウドへ適用していく。また、対策ツールを導入して終わりではなく、ツールの適切な最新化も利用者側での実施が求められる。もし、マルウェアの検出があった場合には、本当に感染したかどうかの確認から、発生源特定、ログの退避、サービスセグメントから感染箇所の切り離し、感染範囲の確認など、早急な一次対処が求められる。このように、マルウェア感染時には早急な対応が求められるため、手順に迷いがないように、事前に調査の手続きを取り決めておく。次いで、感染範囲に対して、被害状況の調査と、どこにどのような報告をしないといけないかの手続きも決めておく。

C4-8：脆弱性対策

設計や設定上のミスや弱点が脆弱性の定義である。攻撃者は、常に新しい攻撃方法を編み出し、システムへ攻撃を仕掛けてくる。利用者は、システムを稼働させるオペレーティングシステムの運用責任があるため、脆弱性への対策を求められる。しかしながら、攻撃方法は進化するため、個別具体的な対応を一つ一つ考えるのは現実的ではない。そもそもは、ミスや弱点が発生しない仕組みを設計時点で織り込んでおく必要がある。加えて、クラウド事業者の支援のもと、オペレーティングシステムの更新とセキュリティパッチの適用も、利用者側での実施が求められる。これらを踏まえて、技術的脆弱性対策の指針と、管理方針の手順の策定が必要とされる。

C4-9：暗号化対策

データの暗号化は、データの重要性やパフォーマンスへの影響を考慮した上で実施する。データの保存や取り扱い時に暗号化を施す仕組みを、実現しているクラウドサービスは各種ある。採用するクラウドのサービスでの暗号化の適用範囲や強度、方式を確認し、システムの要件を満たしているかを確認後、設定を適用する。また、使用する暗号鍵の堅牢な管理はセキュリティ対策の根幹に関わるため、紛失や破壊、漏えい

を防止する対策を講じておく。暗号鍵の管理・保管は、システムの要件に応じて、クラウド事業者側で実施するか利用者側で実施するかを選択する。暗号鍵の紛失や破壊、漏えいまたは、定期的な暗号鍵の更新により、暗号鍵を変更したい場合に備えて、暗号鍵を利用している箇所と、変更時に発生するサービス影響と変更手順を明らかにしておく。

C4-10：ネットワーク対策

クラウドの利用では、オープンなネットワークを情報が通過するため、どのようなシステムにおいても、ネットワークにおけるセキュリティ対策は必須の要件である。また、システムを配置するクラウドの各種エンドポイントおよび内部ネットワークにて、侵入の検知や遮断ができる仕組みを講じる必要がある。具体的にはクラウドとの通信は SSL や TLS といった暗号化通信を前提とし、クラウドの入口箇所にて、ファイヤーウォールや IDS（不正侵入検知システム）、IPS（不正侵入予防システム）などを設置する。これらの設置に伴う設計やバージョンアップ時での更新の手続きを明らかにしておく。

C4-11：アクセス制御

システムにて、ユーザー認証とアクセス認可を設定するが、クラウドの利用でも同様に認証と認可を設定する。特に、クラウドサービスでの認可はサービス毎に細微な設定が可能であり、どのようなアクセス形態にも対応できるようになっている。しかしながら、対応方法が細かいために、設定方法を熟知しておかないと、設定内容にセキュリティ的な不備が発生する可能性がある（AWS ではデフォルトは最小権限、つまりデフォルト権限なしという思想で作られている）。また、インターネット経由で利用するクラウド環境の特性から、サービスによっては、ネットワーク設定でアクセスを制限できない場合がある。このため、利用するユーザーの定義とアカウント設計、クラウドサービス上での設定方法の明文化が重要となっている。クラウドでの各サービスがどのようなアクセスコントロールができるかを把握し、どのような人やシステムが、どのような範囲でサービスを利用するかのアクセス権とロール制御を設計する。設計したアカウント情報をクラウドの各サービスにて設定するが、設定後の動作検証は必須で実施する。システムへのログインが伴う箇所では、パスワードポリシーを設定し、脆弱性につながる要因を排除する。また、利用者の退職や部署異動、セキュリティ障害に備えて、アカウント認証/認可の変更手続きを明らかにしておかなければならない。管理者権限のアカウントでは、コストも含めて、サービスのフルコントロール権限があるため、多要素認証やパスワードの強化、使用状況の監視が求められる。これらを踏まえて、利用するアカウント管理（登録、変更、削除）の全般の運用を設計と手順を定義する。

C4-12：ログ管理

各種サービス利用の証跡はログに記録される。運用するシステムでのセキュリティ要件に照らし合わせて、取得するログの種類、取得範囲、項目、頻度、保存期間を明確にし、トレーサビリティが実現できるように、設計と設定を実施する。また、ログには重要な情報も保存される場合があるため、適切なアクセス権限の設定も重要となる。

C4-13：バックアップ管理

万一の障害や人為的ミスに備えて、システム上で扱うデータやアプリケーションのバックアップを取得する。システム単位での障害だけでなく、リージョン単位やクラウドサービス全体の障害も必要に応じて対象とする。対象となる資産を特定し、資産の重要度を勘案し、目標復旧時点（RPO）と目標復旧時間（RTO）を定義の上、取得頻度や世代管理、暗号化のバックアップ設計を検討する。また、バックアップ取得は目的ではなく、RPO と RTO を守れるかどうかが重要なため、バックアップデータのリストア方式定義と、定期的な訓練計画も求められる。

C4-14：ライセンス管理

利用したいソフトウェアをクラウド事業者が提供していない場合、クラウド事業者のマーケットプレイスにて調達が可能なライセンスを購入するか、利用者が独自にライセンスを持ちこむ必要がある。利用するソフトウェアの使用許諾内容を確認し、利用形態が違反してないかを確認する。その上で、課金体系や、買い切り/サブスクリプションや、固定/フローティング、ダウングレード/アップグレード権などのライセンス形態、サポート条項（日本語での問い合わせ可か）、モビリティによる既存のライセンスの移管の是非などを調査する。また、採用したライセンスは台帳にて一元管理し、利用者の把握と開始日・終了日、金額、資産管理番号など、資産管理としてのライセンス管理が求められる。台帳を最新化するために、定期的なライセンスを棚卸しし、ライセンスを超えた利用をしていないか、不要なライセンスが存在しないかを確認する。

C4-15：構成管理

構成管理では、現時点でのスナップショット以外に、過去の構成情報や検証環境を生成するためのイメージを管理する。また、構成自体以外に、アプリケーションや設定を、サーバインスタンス内へ配置する場合での計画と手続きも管理対象である。管理対象物は構築・開発するアプリケーションやクラウドインフラストラクチャの設計や設定情報である。これらの正確な構成情報をツールで管理する。ツールの利用では、ツール利用の権限と構成変更の際にログを取得し、不正な操作がないかを監査する仕組みが求められる。

4.6 AWS サービス

AWS にはデータやアカウントを保護するために様々なサービスが提供されている。保護自体のサービスもあれば、セキュリティに問題がないかを継続的にモニタリングする仕組みも提供されている。

https://aws.amazon.com/jp/products/security/に、セキュリティ関連のサービスがまとめられているが、それらも含めて各種サービスの概要を以下に示す。

AWS CloudTrail

AWS CloudTrail は、AWS リソースやアカウントの操作をロギングする。利用者のマネジメントコンソールへのサインインや、リソースの追加/変更など、API 操作を伴うアクションもロギングの対象である。ロギングされたログファイルは、暗号化後、S3 に保存される。他サービスと連携し、特定イベント発生時にリアルタイムでの通知が可能であり、不審な操作やルートアカウントへのログイン、セキュリティグループ変更など、セキュリティ的に脅威となる特定の操作を把握できる。

AWS Config

AWS Config では、AWS リソースの設定の評価、監査ができる。AWS リソースの設定変更を継続的にモニタリング・記録でき、以前の状態からの変更を検出しての通知が可能である。また、Config ルールという AWS リソースの設定内容を評価する基準の設定により、実際の AWS リソースの内容との比較評価が自動的におこなわれ、継続的な監査および評価を可能とする。AWS Config の活用により、設定変更全般の確認や、基準との比較が実現でき、継続しての全体的なコンプライアンスの監査および評価が可能となる。

AWS Budgets

AWS は基本的に従量課金のサービスであり、適切に利用しなければ、予算を超過する可能性がある。AWS Budgets により、コストや使用量、Reserved Instance や Savings Plans の利用率・カバレッジが監視できる。コストや使用量の閾値設定に対して超過のチェック通知が可能である。また、傾向からのコスト予測から、予算超過の懸念がある箇所を洗い出し、事前にコスト低減の対策ができる。

AWS Cost Explorer

AWS Cost Explorer は、コストと使用状況の表示と分析が可能である。サービス・リージョン・課金要素・タグなど、様々な視点での料金のグルーピングやフィルタリングにより、料金の傾向分析が可能である。また、Reserve Instance・Savings Plans の購入、適切なサイズのインスタンスタイプへの変更の推奨も受けられる。

AWS Security Hub

AWS Security Hub の利用により、AWS のセキュリティステータスの包括的な管理が可能となる。AWS のセキュリティサービスである、Amazon Inspector や Amazon GuardDuty、Amazon Macie など、セキュリティサービスが検出した Findings 情報を、AWS Security Hub の 1 つの画面で可視化できる。また、一部のサードパーティソリューションとも統合ができるため、ダッシュボード的に様々なセキュリティ側面からの相関的な分析が可能である。加えて、業界標準やベストプラクティスに準拠しているかどうかの自動チェックも可能である。AWS アカウントまたはリソースのいずれかが業界標準やベストプラクティスから逸脱している場合には、その問題にフラグを付け、改善手順を案内してくれる。

AWS Trusted Advisor

AWS Trusted Advisor は、AWS 環境を 5 つの観点で分析し、ベストプラクティスを維持するための改善レポートを提供する。5 つの観点は「コスト最適化」「パフォーマンス」「セキュリティ」「耐障害性」「サービス制限」である。例えば「セキュリティ」では、セキュリティリスクのある設定かどうかのチェックが可能であり、チェック結果はダッシュボードのほか、メールや CloudWatchEvents で通知できるため、素早い検知が可能となる。また、現在よりもセキュリティを高められる推奨の設定をレポートも可能であり、ベストプラクティスに沿って AWS を活用できているかどうかを効率的にチェックできる。（※AWS Trusted Advisor におけるセキュリティについてのチェックのすべてを実施したい場合には、AWS Support にてエンタープライズサポートへの加入が必要となる）

Amazon GuardDuty

Amazon GuardDuty は、悪意のあるアクティビティや不正な動作を継続的にモニタリングし、自動的に脅威を検出する。「AWS CloudTrail のイベントログ」「Amazon VPC フローログ」「DNS ログ」をもとに、既知の悪意のある IP アドレスやドメインなどの脅威を、機械学習や AI を使用して正確に分析・識別し脅威を検出する。脅威が検出されるとダッシュボードなどに、詳細なセキュリティの検出結果が配信される。

Amazon Detective

Amazon Detective は、潜在的なセキュリティ問題や不審なアクティビティの根本原因を分析するためのツールである。「AWS CloudTrail ログ」「Amazon VPC フローログ」「Amazon GuardDuty」を自動的に収集し、機械学習、統計分析、グラフ理論から、セキュリティ調査と視覚化を提供する。セキュリティインシデントの調査プロセスが簡素化され、より迅速かつ効果的な調査を支援する。

AWS Artifact

AWS Artifact には、AWS のインフラストラクチャやサービスについて、「ISO」「PSI」「SOC」などの第三者による監査レポートが保存されている。AWS サービスのセキュリティとコンプライアンスの安全性・健全性を確認できる。また、AWS サービスを利用したシステムの監査や各種認証機関の審査を受ける際、監査レポートを監査人への共有も可能である。

AWS Support

AWS Support は、広義には「AWS サポート」および「Personal Health Dashboard」「Trusted Advisor」などのサービスの総称である。ここでは「AWS サポート」のみ言及する。AWS サポートには、無償の「ベーシック」および有償の「開発者」「ビジネス」「エンタープライズ」の各プランがある。有償プランの利用により、AWS サービス利用時のセキュリティやその他の不安の解消が期待できる。無償の「ベーシック」では、AWS アカウントの利用開始方法や請求、およびサービス制限の緩和申請の問い合わせが可能である。AWS サービスの利用方法やトラブルシューティングなどの技術サポートを受けるには、有償の「開発者」「ビジネス」「エンタープライズ」のいずれかの契約が必要である。「開発者」「ビジネス」「エンタープライズ」の順に、提供されるサポートレベルが高く設定されている。

AWS Shield

AWS Shield は、DDoS 攻撃（分散型サービス不能攻撃）からの保護を提供するサービスの総称である。AWS Shield には「Shield Standard」と「Shield Advanced」の 2 つのレベルがある。Shield Standard は、AWS サービスに組み込み済みの DDoS 攻撃緩和機能であり、無償で利用できる。L3/L4（ネットワークインフラストラクチャ層）に対する DDoS 攻撃の多くから保護ができる。Shield Advanced は、Shield Standard の機能に加えて「L7（アプリケーション層）の DDoS 攻撃からの防御」「AWS の DDoS 対応チームによる 24 時間 365 日サポート」「DDoS 攻撃によって発生した AWS リソース増強に伴うコスト肥大化からの保護」などを提供する有償サービスである。DDoS 対応チームによる対応は DDoS 攻撃発生時のみに留まらず、事後分析や再発に備えた設定支援など、DDoS 攻撃対策全般をサポートしている。

AWS WAF

AWS WAF は、Web アプリケーションへの不正アクセスや脆弱性を狙った攻撃を保護する。マネージドなサービスであり、初期費用不要、インフラストラクチャの管理不要といったメリットがある。AWS WAF では、条件に合致した Web アプリケーションへのアクセスを「許可」または「拒否」することができる。ルールには「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攻撃パターンに合致する」といったものや、「特定の国からのアクセス」「指定した IP アドレスリスト」「ヘッダーやクエリーに含まれる文字列」などの条件の指定ができる。また、AWS およびサードパーティーから「マネージドルール」が提供されており、アプリケーションやサーバーの特性に合わせたルールを設定なしに導入もできる。マネージドルールは、新たな脆弱性や脅威に対処するアップデートが自動的に適用される。

AWS Certification Manager

AWS Certification Manager（ACM）は、SSL/TLS 証明書の発行・管理を提供する。SSL/TLS 証明書は、事業者へ証明書発行を依頼するが、費用がかかり、申請・審査・発行の手続きに数日間の期間を要する。ACM では「AWS の特定サービス（Elastic Load Balancer、CloudFront など）で利用する」という条件があるものの、無償で SSL/TLS 証明書が数時間で発行が可能である。また、ACM の証明書は自動更新のため、再発行や入れ替えの手間から解放される。ACM では、インターネットに公開する際に用いる「パブリック証明書」の他に、自社・自組織内で利用するための「プライベート証明書」の発行もできる。

Amazon Inspector

Amazon Inspector は、EC2 への意図しないネットワークアクセスや、EC2 の脆弱性をチェックし、自動的なセキュリティ評価を可能とする。例えば、「インターネットから EC2 にアクセス可能になっていないかどうか」や「リモートルートログインが有効になっていないかどうか」「脆弱なソフトウェアがインストールされていないかどうか」など、セキュリティの脆弱性やベストプラクティスから逸脱していないかを評価し、逸脱している項目の報告が受けられる。

AWS Systems Manager

AWS Systems Manager は、AWS リソースを一元的に表示および管理でき、AWS リソース全体の運用タスクを自動化できる。AWS Systems Manager は運用に関連する様々な機能を持っている。ブラウザベースのシェルおよび CLI の提供や、OS とソフトウェアのパッチの自動デプロイなどがある。安全で効率的に定型的な運用タスクの自動化の作り込みが可能となる。

Amazon CloudWatch

Amazon CloudWatch は AWS のリソースやアプリケーション、オンプレミスのサーバーをモニタリングする。ロギングされたデータの中から特定の文字列を含むデータを抽出し、発生頻度をグラフで可視化したり、閾値を超えた場合に通知が可能である。他のサービスと組み合わせにより、セキュリティリスクのあるリソースの操作があった場合に迅速な検知が可能となる。

Amazon CloudWatch Logs

Amazon CloudWatch Logs は AWS サービスおよび顧客システムのログの監視、保存、アクセスを提供する。特定の文字列がロギングされた場合にメトリクスとして値をカウントし、閾値を超えた場合に通知する機能があり、不審なアクティビティを検出した場合に、メールなどへ通知できる。

AWS License Manager

AWS License Manager では、多様（Microsoft,SAP,Oracle,IBM）なソフトウェアベンダーのライセンスを一元管理できる。組織でソフトウェアライセンスがどのように使用されているかを可視化および制御でき、あらかじめ作成したカスタムライセンスルールを使用し、ライセンス超過による契約違反、申告ミス、コスト増加のリスクを軽減できる。

Amazon CodeGuru

Amazon CodeGuru は、機械学習を利用してコードに欠陥がある部分を特定し、改善方法を含め、推奨事項を生成する開発者向けのサービスである。例えばクレジットカード番号などをログに出力していないかなど、機密情報の漏洩リスクが検知できる。アプリケーションロジックでの機密情報の漏洩や攻撃を未然に防ぐことが可能となる。

AWS Secret Manager

AWS Secrets Manager は、シークレットを安全に管理する（ここでの「シークレット」とは、データベース認証情報、パスワード、サードパーティーの API キーなどの情報を指す）。アプリケーション内にシークレットをハードコードする必要がなくなり、シークレットが必要な部分を API に置き換えるだけで、アプリケーションは安全にシークレットの取得が可能となる。

AWS X-ray

AWS X-ray は、アプリケーションが処理するリクエストに関するデータを収集する。レスポンスタイムやステータスなどを収集し、表示、フィルタリング、分析、デバッグが可能である。マイクロサービスアプリケーションにおいて把握が難しいサービス間の依存関係を可視化し、エラーの原因となるサービスやパフォーマンス上のボトルネックを発見に役立てられる。また、アプリケーション全体で転送されるユーザーリクエストがトレースでき、アプリケーションを構成する個々のサービスやリソースによって生成されるデータが集計されるサーバレスアプリケーションやコンテナにおける障害対応・パフォーマンス分析が容易に可能である。

AWS Backup

AWS Backup により、AWS リソースのバックアップを一元管理できる。ディスクやデータベースなどを対象にバックアップのスケジューリング・保持管理・モニタリングおよびアラートの設定ができる。また、バックアップを複数の異なる AWS リージョンにオンデマンドでコピーできるため、ビジネス継続性またはデータ保管のコンプライアンス要件へ容易に対応できる。

AWS Identity and Access Management

AWS Identity and Access Management（IAM）は、AWS における認証と認可を担う。AWS 上でシステムの開発や運用を担うメンバーを識別するためのユーザーを発行することができる。また、各ユーザーに対して認証のためのパスワードや追加の認証要素（ワンタイムパスワードなど）が設定できる。各ユーザーに対してはカスタマイズした権限を付与できる。AWS に対する権限は、ユーザー以外（API など）にも付与することが可能である。IAM Role を利用することで、AWS サービスやほかの AWS アカウント、外部の認証プロバイダーに対して権限を委任することも可能である。

AWS Single Sign-On

AWS Single Sign-On（AWS SSO）は、複数の AWS アカウントおよびビジネスアプリケーションへのシングルサインオンアクセスの一元管理を可能にする。AWS SSO では、AWS Organizations のアカウントに対するアクセスとユーザーアクセス許可を簡単に一元管理ができるため、煩雑になりがちなアカウント管理をシンプルな運用に置き換えることができる。結果、アカウントへの統制が高まり、セキュリティ性が向上する。

AWS IAM Access Analyzer

AWS IAM Access Analyzer は、所有する AWS アカウント外に対して付与している権限を検査・管理できる。AWS では、IAM で管理するユーザーやロールなどのエンティティだけでなく、リソースにもポリシーを付与できる。このリソースポリシーを通して、AWS 上のリソースの公開や、他の AWS アカウントからのアクセス許可が可能である。

AWS Key Management Service

AWS Key Management Service（KMS）では、データの暗号化に使用する暗号鍵の作成と、暗号鍵の一元管理ができる。暗号鍵は KMS で作成するほか、作成済みの暗号鍵のインポートも可能である。IAM ユーザー/ロールに対して KMS の管理や、暗号鍵の使用に認可を与えることも可能である。また、AWS の多様なサービスと連携して、データ保管時の暗号化に KMS で管理されるカスタマーマスターキー（CMK）を利用可能である。カスタマーマスターキーは利用者側で管理出来るため、クラウド上にデータを保管する際のコンプライアンス対応や、データの消去の代わりに、鍵を破棄ことでの対応が可能である。

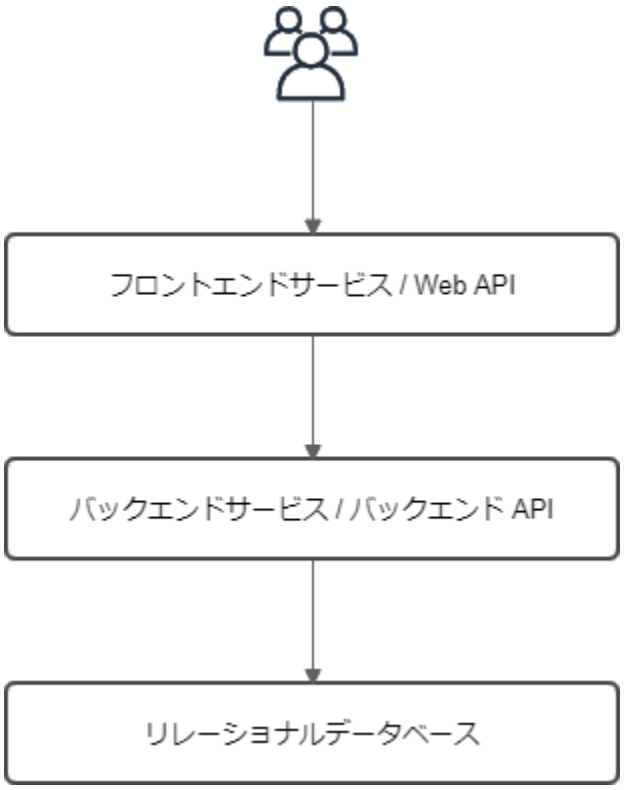
AWS CloudHSM

プラットフォーム内の重要なデータの保護のため、データを保護する暗号キーの管理において、米国政府標準規格などへの適合が求められる場合がある。AWS CloudHSM により、安全なキーストレージや高パフォーマンスの暗号化オペレーションを AWS アプリケーションに簡単に追加できる。AWS CloudHSM はクラウドベースのハードウェアセキュリティモジュールであり、不正使用防止策の施されたハードウェアデバイス内で、安全なキー保管と暗号化操作を可能とする。暗号キーデータを安全に保存し、ハードウェアの暗号境界の外側からは見えないようにして、キーデータの利用が可能である。

5 設計例

この章では、AWS における典型的な構成のシステムに対して各種セキュリティ対策を施した例を紹介する。

今回は、以下のような三層アーキテクチャのシステムを例に挙げる。



今回、設計例を以下の 3 つの設計要素に分けて説明する。

- ネットワーク
- サーバー
- AWS アカウント

なお、設計対象のシステムは以下のような仕様であると仮定する。

- 物理サーバーもしくは仮想サーバー上での動作がサポートされている一般的な Web アプリケーション
- リレーショナルデータベースをサポートしている

また、設計にあたっては以下のような要件を満たせることを目指す。

カテゴリ	要件	対応サービス
クラウド構築検討	単一障害点を排除したい	AmazonNirtual Private Cloud（Multi-AZ）
クラウド運用検討	システム管理者によるアクションが必要な事象（非障害）の発生を認識したい	AWS Health
サービスリソースにかかる運用作業	パフォーマンスを分析したい	Amazon RDS（Performance Insights）、Amazon CloudWatch
システム監視	システム管理者によるアクションが必要な事象（障害）の発生を認識したい	CloudWatch、Amazon Route53（Health Check）、Amazon SNS、AWS Chatbot
コスト管理	予算を超える利用を把握したい・予見したい コストの削減などを意図して利用料金を分析したい	AWS Cost Explorer、AWS Budget
新規サービスの検討	ー	
マルウェア対策	ー	
脆弱性対策	各レイヤーにおける脆弱性を検知したい ソフトウェアの脆弱性を速やかに修正したい	Amazon Inspector、AWS Systems Manager（Patch Manager）
暗号化対策	保存されているデータを暗号化したい 暗号化のための鍵を厳格に管理したい	AWS Key Management Service
ネットワーク対策	通信を暗号化したい 不正なアクティビティを検知・防御したい ネットワークアクセスの許可を最小化したい	Amazon Certificate Manager、Amazon GuardDuty、AWS Shield、AWS WAF、Amazon VPC（セキュリティグループ、ルートテーブル、サブネット）
アクセス制御	適切な認証強度のユーザー認証を行いたい ユーザーに対して詳細なアクセス許可を付与したい 不正なアクティビティを検知したい 不必要なアクセス許可を検知したい	AWS IAM、Amazon GuardDuty、AWS IAM Access Analyzer
ログ管理	システム上のアクティビティを把握する為に必要なログを取得したい ログを適切な期間保存したい ログを分析したい	AWS Systems Manager（Session Manager）、Amazon Simple Storage Service (Amazon S3)、Amazon CloudWatch Logs、Amazon Athena
バックアップ管理	アプリケーションで取り扱うデータを適切にバックアップしたい	AWS Backup
ライセンス管理	システム上で利用しているソフトウェアを把握したい	AWS Systems Manager（Inventory）
構成管理	システムの構成変更を継続的に記録したい リスクのある設定を検知・是正したい	AWS Config、AWS Security Hub

5.1 ネットワーク

5.1.1 ネットワーク設計

AWS では、論理的に独立したネットワークを提供する Amazon VPC を提供している。

Amazon VPC は、以下のような様々なコンポーネントを提供している。

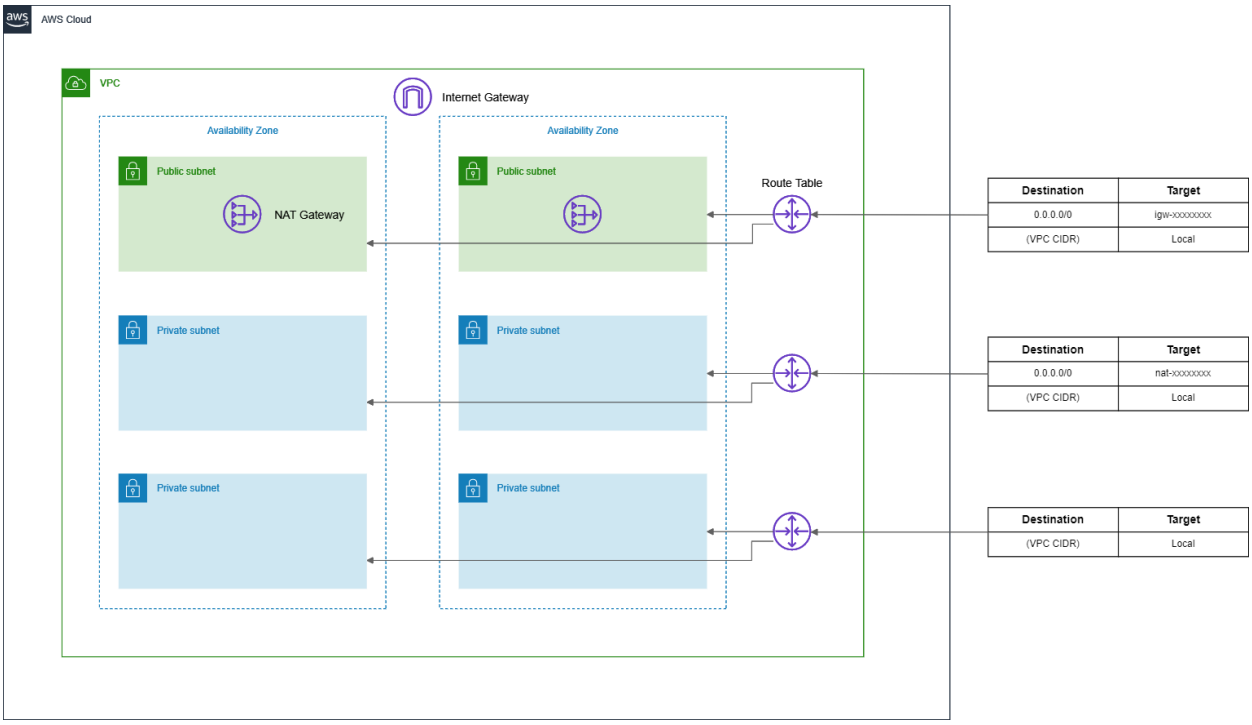
- VPC・・・論理的に独立したネットワーク空間
  - AWS が提供する各リージョンに作成できる
- Internet Gateway・・・VPC と Internet を接続するための仮想ゲートウェイ
- Virtual Private Gateway・・・VPC とオンプレミスのネットワークを接続するための仮想ゲートウェイ
- Subnet・・・VPC のネットワーク空間を分割するリソース / 特定の Availability Zone に作成
  - Availability Zone（以下、AZ）・・・AWS サービスを提供するリージョンに存在するデータセンター群 / リージョンは基本的に複数の Availability Zone で構成される / AZ の間には一定の距離があり、複数の AZ に跨がってサーバーを展開すると高い可用性のシステムを構成できる
- Route Table・・・ルーティングを制御するリソース
- Security Group・・・ネットワークアクセス制御を行うリソース

これらのコンポーネントを利用することで、VPC においてインターネットから直接アクセスできるネットワーク（DMZ）とプライベートなネットワークを定義できる。

今回の設計例では以下のサブネットを定義する。

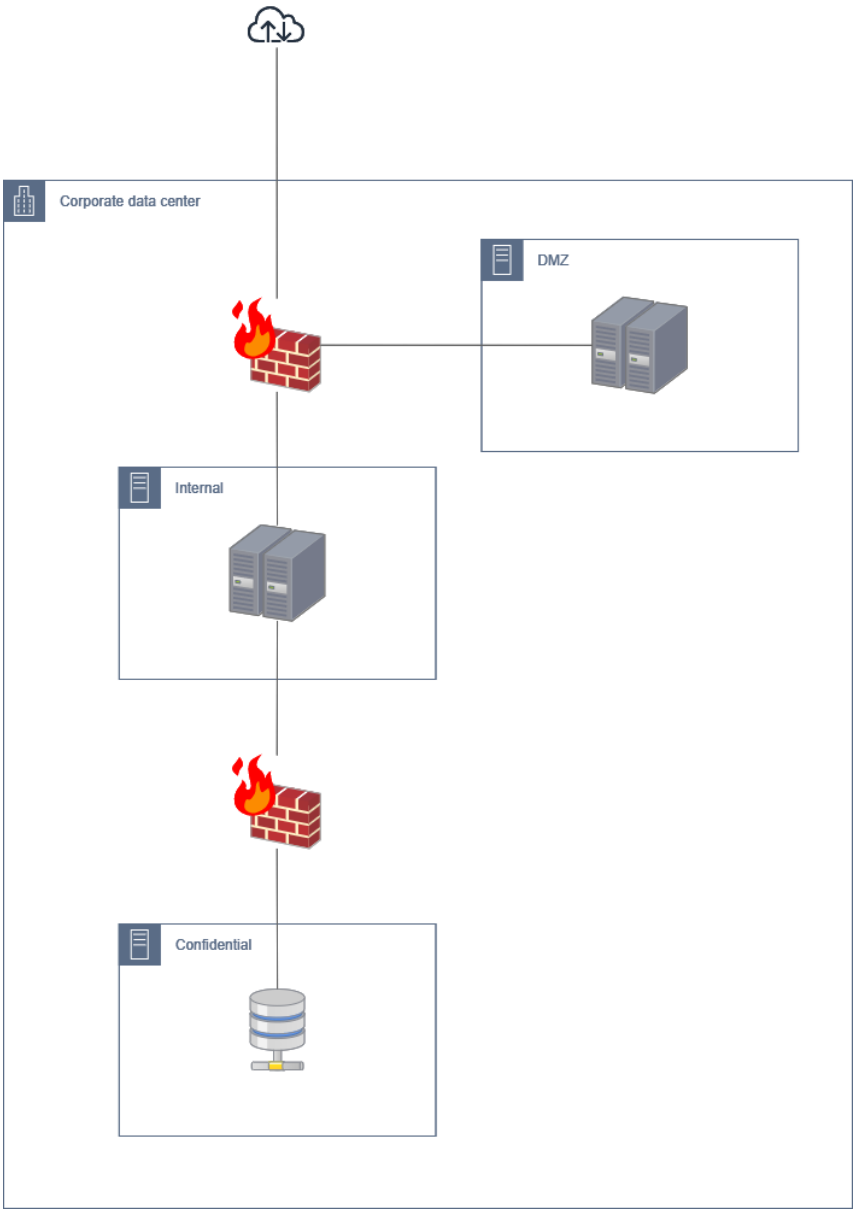
- Public Subnet
  - インターネットに直接ルーティング可能
- Private Subnet
  - NAT Gateway (https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html) 経由でインターネットへのアウトバウンド通信は可能。（パッチのダウンロードなどの用途を想定）
- Data Subnet
  - VPC 外部と通信できない

VPC で複数の AZ に Subnet を作成しておき、サーバー群を分散配置することで容易に冗長化を実現することができる。今回の例では 2 つの AZ に Subnet を作成している。



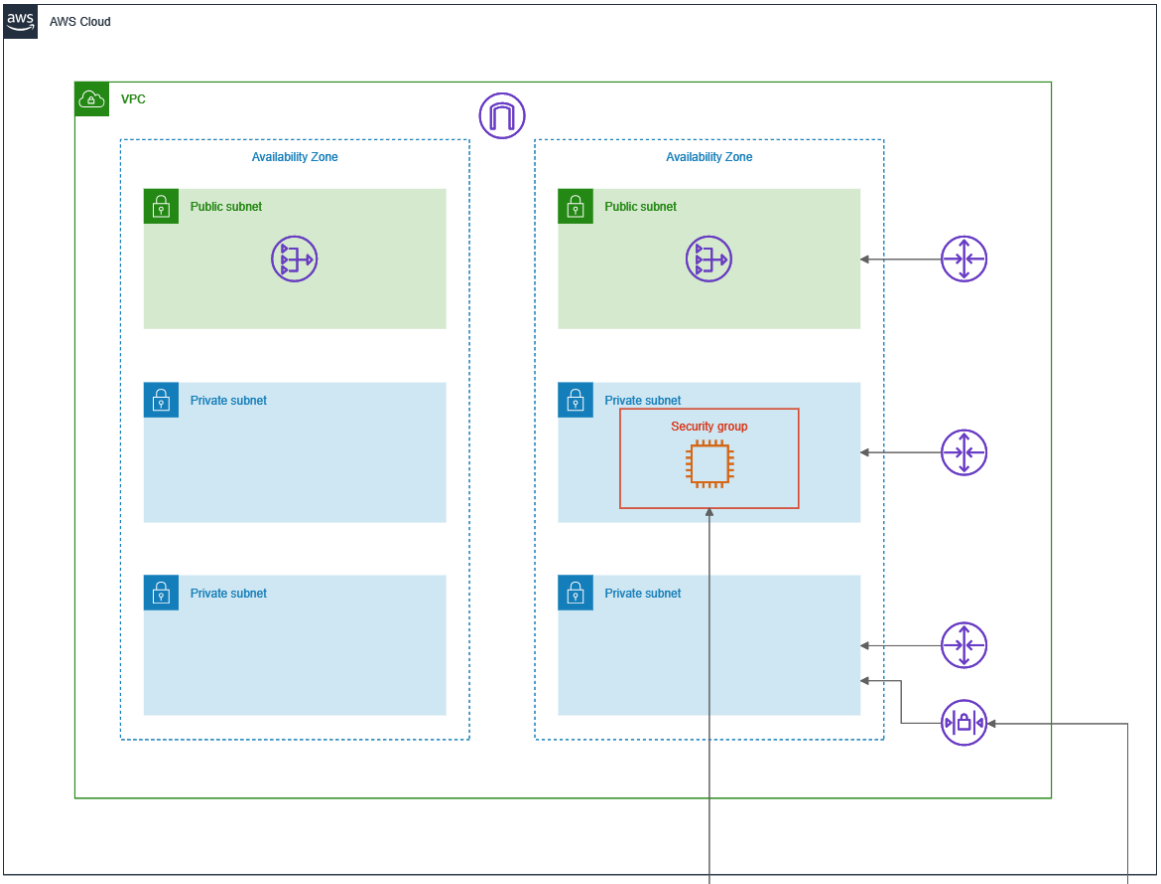
ここで、従来のネットワーク設計に慣れている方は、「ネットワークアクセス制御はどうするのか」「DMZ をどのように構成するのか」といった疑問を持つかもしれない。

従来のネットワークでは Firewall としての役割を有する機器を中心にした境界型のアクセス制御が一般的である。しかし、前出の図ではそういったコンポーネントは表現されていない。


Corporate data center
DMZ
Internal
Confidential

AWS においては Security Group および NACL を利用してアクセス制御を実現できる。Security Group は、VPC 上に構成できるリソースに割り当てられるネットワークインターフェースに対して適用される。つまり、ゲートウェイではなくエンドポイント側でアクセス制御が行われる。

また、NACL（Network ACL）を用いたアクセス制御も可能である。NACL は Subnet に対して割り当てることでそのルールをネットワークに適用できる。



Security Group

Type	Protocol	Port	Source
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

Network Access Control List

Rule	Type	Protocol	Port	Source	Allow / Deny
100	SSH	TCP	22	0.0.0.0/0	DENY
200	ALL TCP	ALL	ALL	0.0.0.0/0	ALLOW

5.1.2 サーバーの配置

ネットワークを構成したら、サーバーをどのように配置を検討する。

AWS において汎用的な仮想サーバーを利用したい場合、Amazon EC2 を利用することができる。Amazon EC2 は、仮想サーバーに相当する EC2 インスタンスを提供することが主たる機能である。サービスを利用するにあたりホストサーバーやハイパーバイザーを意識する必要は無い。

また、リレーショナルデータベースを利用したい場合には、Amazon RDS を利用することができる。Amazon RDS は、データベースエンジンが構成済みの RDS インスタンスを提供する。Amazon EC2 では「OS・データベースエンジンの設定」「バックアップ」「パッチ適用」「ログ管理」「冗長化」などを利用者が管理する必要があるが、RDS ではこれらをサービス内で担ってくれるマネージドサービスである。設計・構築・運用の負担を大幅に軽減することができる。

本設計例では、「フロントエンドサービス」「バックエンドサービス」に Amazon EC2、「リレーショナルデータベース」に Amazon RDS を採用することとする。

サービスに対して一定の可用性を求める場合、各役割のサーバーを冗長化させることが一般的である。

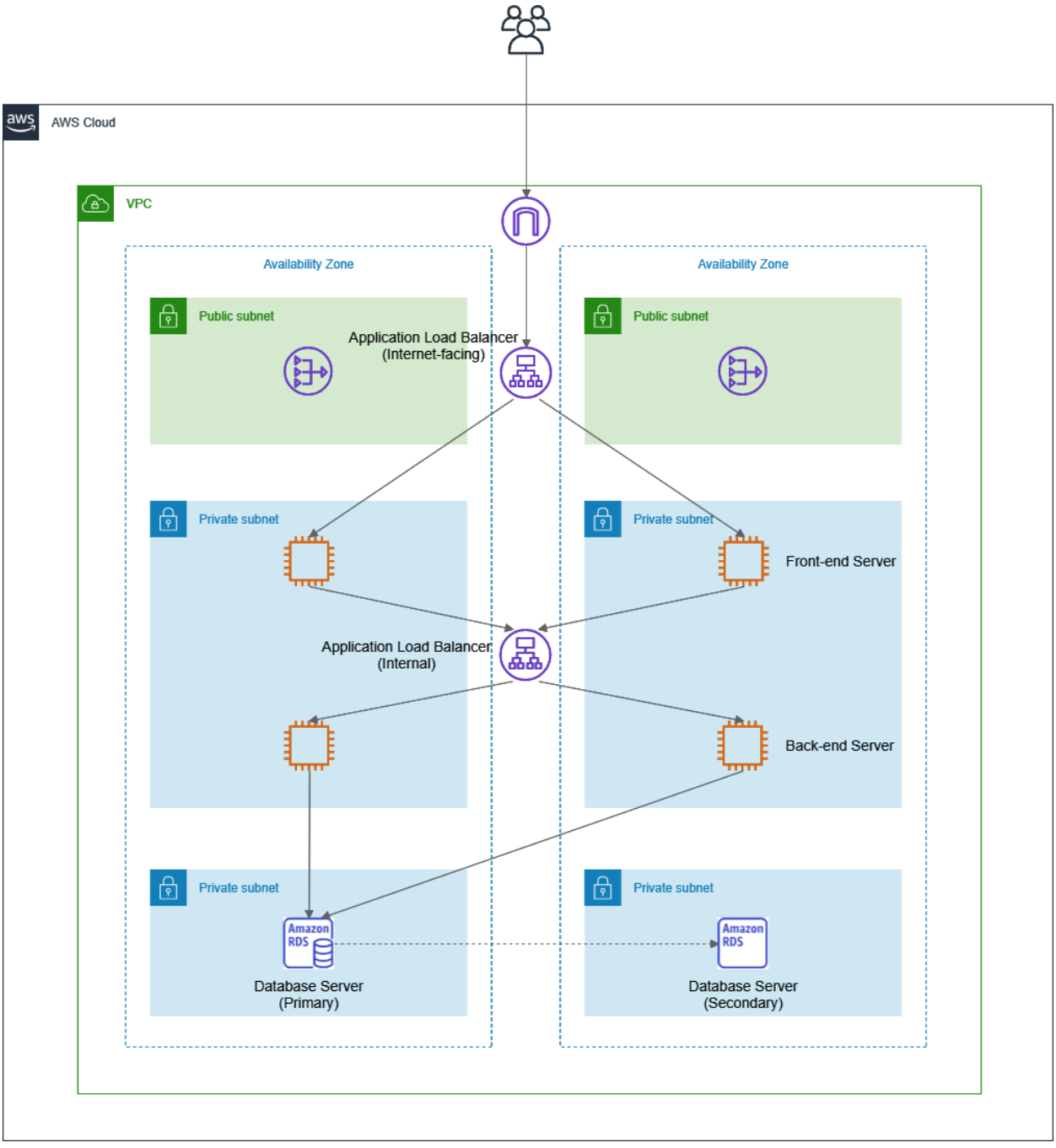
今回は「フロントエンドサービス」「バックエンドサービス」「リレーショナルデータベース」の 3 種類のサーバーを構成する必要があると仮定し、各種類のサーバーを 2 つの AZ に配置することとする。

この際、「フロントエンドサービス」「バックエンドサービス」においては ELB（Elastic Load Balancing）を利用することができる。ELB を利用することで、クライアントがサービスにアクセスするエンドポイントを提供し、異なる AZ に配置されたサーバーへリクエストをルーティングすることができる。

一般的な Web サービス（HTTP/HTTPS）の場合、ALB が適している。

今回の設計例では、「フロントエンドサービス用の ALB」は Public Subnet、「フロントエンドサービスのサーバー」「バックエンドサービス用の ALB」「バックエンドサービスのサーバー」は Private Subnet に配置する。

また、「リレーショナルデータベース」では Data Subnet に配置する。また、RDS のインスタンスを作成する際に Multi-AZ 配置にすることで異なる AZ にマスターおよびスタンバイインスタンスを作成する。



5.1.3 セキュリティ

ここまでのネットワーク設計およびサーバーの配置を前提に各種サービスを利用してネットワークのセキュリティを強化することができる。

ネットワークのセキュリティを強化するために、以下のようなサービスを利用することができる。

- Amazon Route53
- Amazon CloudFront
- AWS Certificate Manager (ACM)
- AWS WAF
- ELB / VPC

Route53 は、ドメインを管理するためのサービスである。ネームサーバーとしての機能以外にヘルスチェックやドメインの取得なども可能である。後述する CloudTrail や IAM を利用することで管理操作の証跡を取得およびユーザー認証の強化を実現することができる。また、ヘルスチェックを利用して Active-Active もしくは Active-Standby の冗長化を行うこともできる。

本設計例では、ドメインの管理とヘルスチェックによるサービスの監視を行うものとする。

CloudFront は AWS の提供する CDN サービスで、サービスを利用するエンドユーザーに近いロケーションにコンテンツをキャッシュし、サービスのパフォーマンスを改善できる。キャッシュを保持していないコンテンツへのリクエストがオリジンへルーティングされるため、オリジンの負荷を軽減することができる。

セキュリティを強化する機能として、「アクセスログの取得」「特定地域からのリクエストをブロック」「カスタムエラーレスポンスの生成（Sorry Page）」などの機能が提供されている。また、CloudFront を利用することで User Datagram Protocol (UDP) reflection attacks や SYN Flood などの攻撃を緩和できる。

本設計では、フロントエンドサービスの ALB をオリジンとする CloudFront ディストリビューションを作成する。また、トラブルシュートやインシデント調査のためにアクセスログの取得、オリジンが正常にリクエストを返せなくなった場合でもクライアントに適切なエラーページを表示させるためにカスタムエラーレスポンスを利用する。なお、Sorry Page のホスティングには S3 を利用することができる。

ACM は、SSL/TLS X.509 証明書の管理を行うサービスであり、このサービスからサーバー証明書を発行することができる。ACM で発行するサーバー証明書は、CloudFront・ELB などと連携することが可能である。

本設計では、ACM で発行したサーバー証明書を CloudFront と連携させ、HTTPS でサービスを提供する。その際、適切なセキュリティポリシー（サポートする SSL/TLS protocol および Cipher のリスト）を選択する必要がある。

WAF は Web アプリケーションファイアーウォールのマネージドサービスである。保護ルールを独自に構成することもできるし、AWS およびサードパーティーから提供されるマネージドルールを利用することもできる。CloudFront・ELB と連携することが可能である。アクセスログを収集し、後で分析することもできる。

本設計では、マネージドルールによる保護およびログの収集を実施する。ただし、Managed Rule において誤検知が発生した場合、ログから誤検知の原因となっているルール ID を特定して除外するなどの運用が必要となるため、運用手順を押さえておく必要がある。AWS は Marketplace などを通してサードパーティーの仮想アプライアンスや SaaS を調達することができる。運用に習熟している場合にはそれらも有力な選択肢になり得る。

すでに言及済みの ELB / VPC に関しても、以下のような機能を利用可能である。

- ELB
  - HTTP Desync
    - HTTP Desync 攻撃を緩和することができる
  - Listener Rule
    - リクエストヘッダーなどに応じてルーティング先・応答内容を指定できる
    - CloudFront でオリジンへの転送時にカスタムヘッダーを追加することで、CloudFront 経由でのリクエストのみに正常な応答をするように構成できる
  - ACM との連携
    - ACM で作成したサーバー証明書を関連付けることで HTTPS Listener を構成できる
      - CloudFront は Origin との HTTPS 通信をサポートできるため、VPC 外の通信を暗号化したい場合にも対応できる
  - Access log

        - ✧ アクセスログを収集できる
- VPC
    - ➢ VPC FlowLogs
        - ✧ VPC 内のフロー情報をロギングできる
    - ➢ DNS Query Log
        - ✧ VPC 内のインスタンスから Amazon Provided DNS への DNS クエリーをロギングできる

各ログのフォーマットを公式ドキュメントで確認することができる。また、ログの種類によっては、出力の頻度やフォーマットを変更することもできる。

例えば、VPC FlowLogs における最大集約期間はデフォルトで 10 分だが、これを 1 分にすることでログ分析のリアルタイム性を向上させることができる。また、デフォルトのフォーマットに対していくつかのフィールドを追加することができる。

また、CloudFront ではリアルタイムでのログ出力をサポートしている。

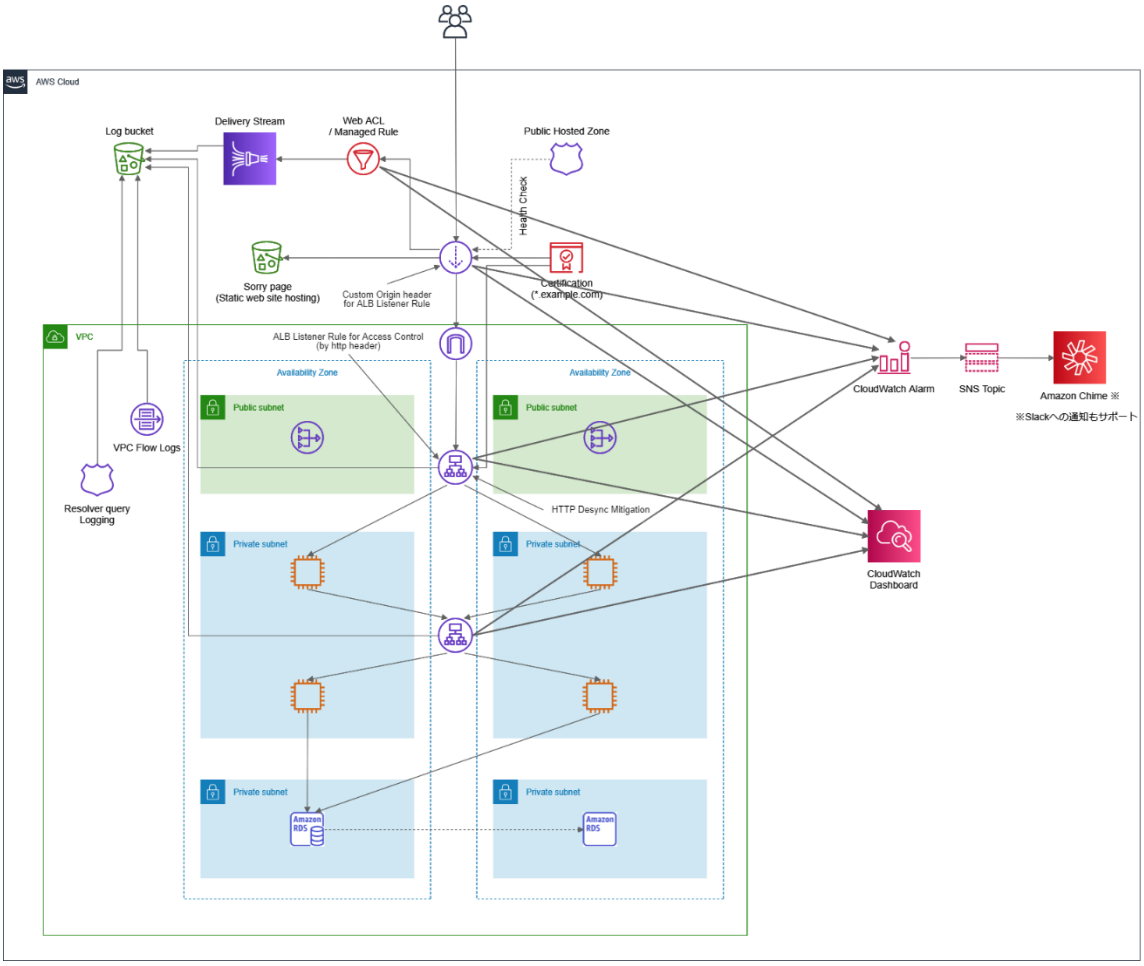
5.1.4 監視

サービスの健全性を監視し、障害発生時には復旧のために迅速かつ適切な対応を実施する必要がある。

AWS では CloudWatch というサービスを利用することで AWS リソースの各種メトリクスを計測および監視することができる。また、Amazon SNS や AWS Chatbot を利用することでメールや一部のチャットサービスにアラートを通知することもできる。

AWS WAF・CloudFront および ELB では、エラーレート・エラー数、レイテンシなど監視することでシステム管理者による調査や復旧が必要なイベントの発生を認識することができる。

併せて、ステークホルダーが現状を正しく認識するために CloudWatch やサードパーティーのサービスを利用してダッシュボードを作成することも有効である。

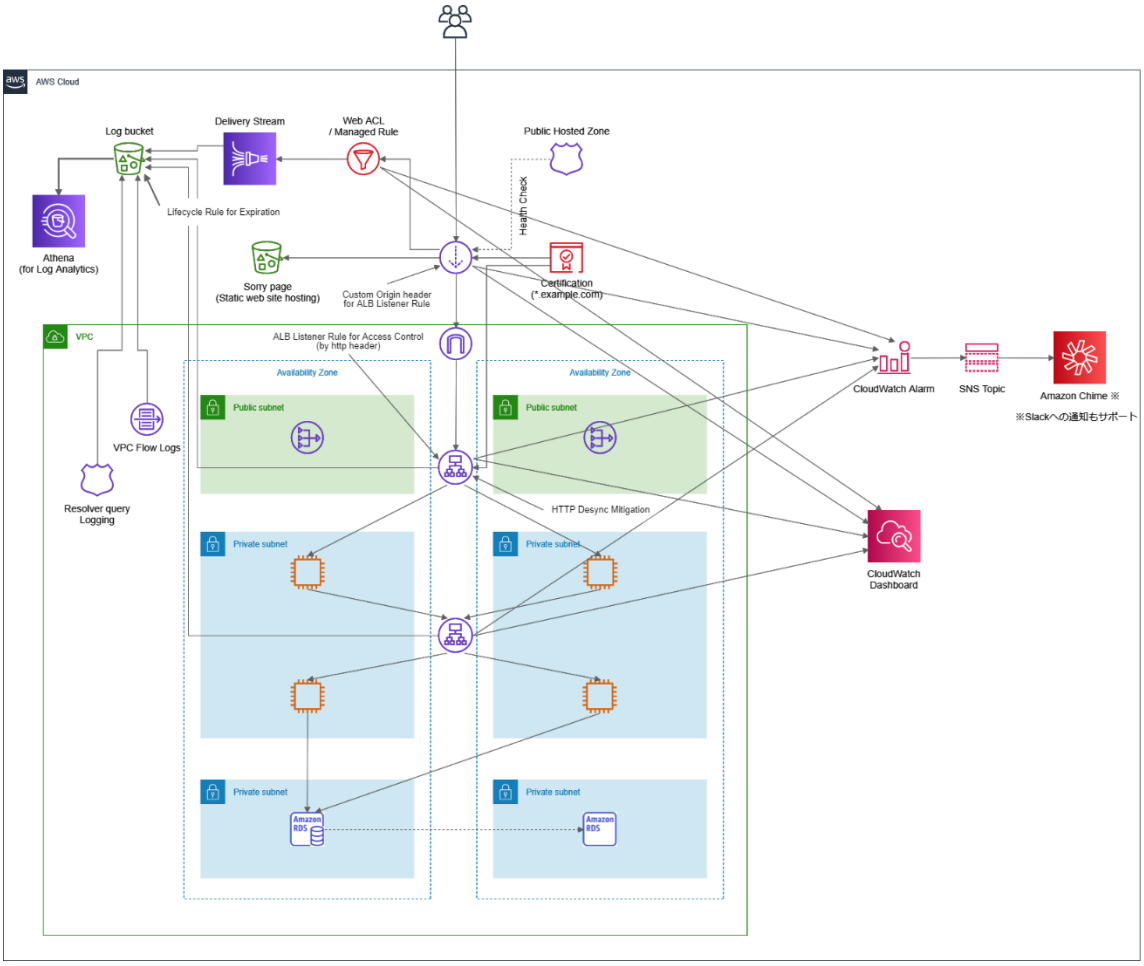


5.1.5 ログ管理および分析

様々な AWS リソースから出力されるログを保存するために Amazon S3 を利用することができる（もう一つの主要な選択肢である CloudWatch Logs は後述する）。Amazon S3 を利用することによって対象のデータを低コストで管理することができる。

ログを管理するにあたり、有効期限を定義して管理することが一般的だが、Amazon S3 ではライフサイクル機能としてオブジェクトの有効期限を設定して削除を自動化することができる。

また、AWS Athena を利用することにより、ログファイルなど S3 にある大量のデータに対してクエリーを実行することもできる。スポットでのログ分析に非常に有用である。


AWS Cloud
Log bucket
Delivery Stream
Web ACL
/ Managed Rule
Public Hosted Zone
Health Check
Lifecycle Rule for Expiration
Athena
(for Log Analytics)
Sorry page
(Static web site hosting)
Custom Origin header
for ALB Listener Rule
Certification
(*.example.com)
VPC
ALB Listener Rule for Access Control
(by http header)
Availability Zone
Availability Zone
Public subnet
Public subnet
VPC Flow Logs
Resolver query
Logging
HTTP Desync Mitigation
Private subnet
Private subnet
CloudWatch Alarm
SNS Topic
Amazon Chime ※
※Slackへの通知もサポート
CloudWatch
Dashboard
Private subnet
Private subnet
Amazon
RDS
Amazon
RDS

5.2 サーバー

本章の設計例では、Amazon EC2 および Amazon RDS を利用してサーバーを構成する。本節ではネットワーク上に配置する EC2 インスタンスの構成例を解説する。

なお、Amazon RDS の構成例は本節の最後で EC2 と対比しながら解説する。

5.2.1 サーバー構築

EC2 インスタンスを作成する際、AMI（Amazon Machine Image）を利用して作成する。AMI の提供元を大まかに分類すると以下の通りである。

- AWS
- サードパーティーベンダー
- コミュニティ
  - centos.org / Canonical など提供元がはっきりしているケースとそうでないケースがある
  - 提供元のはっきりしない AMI の利用は推奨されない

一部の AMI はハードニングが施されているものがあり、要件に応じて適切な AMI を選ぶことが望ましい（STIG compliance に対応した Windows Server など）。

また、最新のインスタンスタイプを利用することも推奨される。最新のインスタンスタイプは Nitro Hypervisor 上で動作しており、セキュリティおよびパフォーマンスの面で旧来のインスタンスタイプより優れている。

5.2.2 時刻同期

AWS では、Amazon Time Sync Service として時刻同期サーバーが提供されている。高い可用性および精度で時刻参照が可能である。

これにより、高い精度でログのタイムスタンプの正しさを維持することができる。また、うるう秒への対応も容易に行うことができる。

5.2.3 運用管理

AWS では、AWS Systems Manager を利用することで、運用フェーズで発生するオペレーションの人的負荷を軽減することができる。具体的には、パッチ管理・インベントリ管理・認証情報の管理などを AWS のマネジメントコンソールで手動実行もしくは自動化することができる。各機能の詳細は関連する項で解説する。

Systems Manager を利用するためには EC2 インスタンスに SSM Agent をインストールし、Systems Manager やその他関連するサービスへの権限を有する認証情報を設定する必要がある。なお、IAM Role(Instance Profile)を利用することでインスタンスメタデータから一時的な認証情報を適宜取得することができる。

定型化されていないオペレーションは SSH/RDP などでインスタンスに接続して実行することになるが、Systems Manager Session Manager を利用することでセキュアな運用を実現できる。具体的には、以下のようなメリットがある。

- セッションを開始するには IAM での認証が必要
  - 認証時にパスワードと MFA を利用することができる
  - SSH / RDP 接続のために秘密鍵を利用する必要がない
- セッション開始時のログおよびセッション自体のログを収集することができる

踏み台サーバーおよび管理対象の EC2 インスタンスに対して SSH/RDP のためのネットワークアクセス許可を追加する必要がない

5.2.4 脆弱性管理

Amazon Inspector を利用することで、EC2 インスタンスの脆弱性（OS の設定およびソフトウェアパッケージ）を検出することができる。管理対象の EC2 インスタンスに Agent のインストールと IAM Role などを介した権限の付与を行うことで利用することができる。

複数のルールパッケージが提供されており、脆弱なソフトウェアパッケージの有無・OS 設定・ネットワークアクセス許可・プロセスの起動状況、等を検出することができる。

検出された脆弱性のうち、対策が必要なものは稼働中のインスタンスに対する修正もしくは AMI の更新などを実施する必要がある。稼働中のインスタンスに対してパッチを適用する場合、Systems Manager RunCommand を利用することで多数の対象への一括適用や作業の証跡の管理が容易になる。

5.2.5 暗号化対策

EC2 インスタンスと連携するストレージサービスは複数あるが、最もよく一緒に領されるのが Amazon EBS である。Amazon EBS はブロックストレージのサービスで、EC2 インスタンスからはローカルストレージのように利用することができる。

セキュリティ要件によってはストレージの暗号化を実施する必要があるが、Amazon EBS では AWS KMS を利用してストレージボリュームの暗号化を行うことができる。

5.2.6 認証情報の管理

AWS 上では様々な認証情報を取り扱う。例えば、データベースの接続情報や AWS のアクセスキーなどである。AWS が定義するセキュリティベストプラクティスでは、こういった認証情報をハードコードしてはならないとされている。

AWS の API を利用するための（一時）認証情報は EC2 に IAM Role を割り当てることでインスタンスメタデータから取得することができる。また、データベースへの接続情報は Systems Manager Parameter Store もしくは Secret Manager を利用して管理することができる。

これにより、AMI やアプリケーションリポジトリーに認証情報が含まれることで意図しない認証情報の漏洩リスクを抑えることができる。また、サーバーをスケールアウトする際に設定情報や認証情報の展開を容易に実現できる。

5.2.7 ログ管理

アプリケーション・ミドルウェア・OS などから出力されるログは、トラブルシュートや脅威検知およびアプリケーションの改善などに有用である。

EC2 インスタンス上で発生するログの管理には CloudWatch Logs が利用できる。CloudWatch Agent のインストールおよび CloudWatch Logs へのログの送信権限などが必要となる。

CloudWatch Logs に収集したログに対して、メトリクスフィルタを利用して指定した条件のログ件数のカウントや、CloudWatch Logs Insights によるログの分析を行うことができる。

5.2.8 バックアップ

EC2 インスタンスにおいて起動不能な障害が発生した場合、何らかの方法で復旧する必要がある。EC2 インスタンスが何らかのデータを保持している場合などは EC2 インスタンスをバックアップする必要がある。なお、アプリケーションの設定が完了している AMI を作り込み、なおかつデータはデータベースなどのバックエンドサービスで管理しておけばバックアップを行う必要はない。作り込まれた AMI (Golden AMI) を利用して EC2 インスタンスを復旧すればよい。

AWS では、AWS Backup を利用して EC2 インスタンスのバックアップの取得を自動化することができる。その際、バックアップウィンドウやバックアップデータを保持する期間などを指定することができる。

また、バックアップに失敗している場合に備えて AWS Backup のイベントを通知することが望ましい。

5.2.9 インベントリ管理

EC2 インスタンスで有償のソフトウェアを利用している場合、そのライセンス管理を適切に行う必要がある。

Systems Manager の State Manager および Inventory の機能を利用することで、インストールされているソフトウェアパッケージなどの情報を自動的に収集することができる。

5.2.10 監視

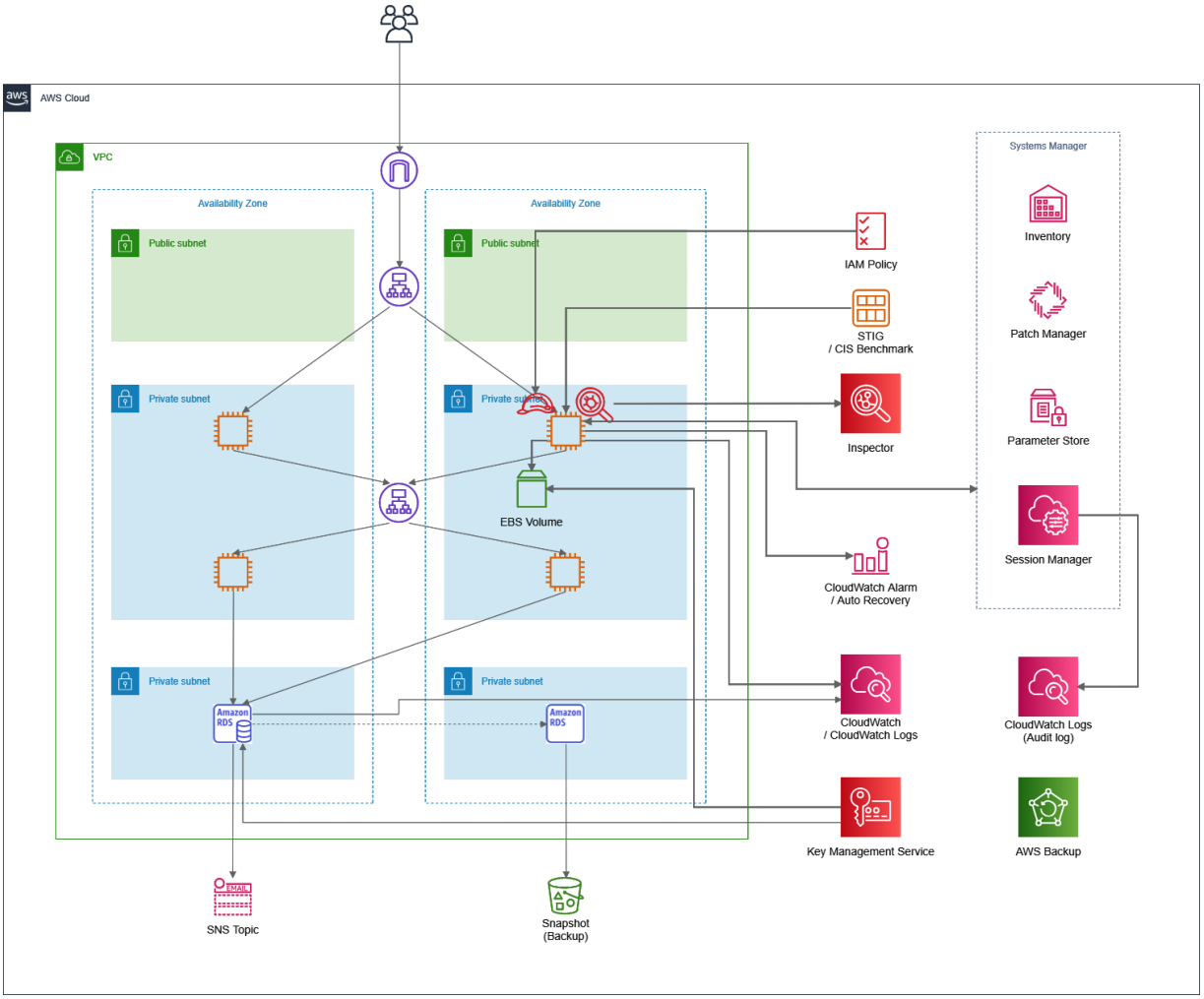
ネットワークリソース同様に EC2 インスタンスに関しても適切な監視が必要である。

EC2 インスタンスも CloudWatch を利用して様々なメトリクスを取得することができる。ただし、標準のメトリクスにはメモリの利用率やディスクの利用率など OS のメトリクスは含まれていないため、必要な場合には CloudWatch Agent などの利用を検討する必要がある。

通知の方法はネットワークリソースの監視同様に CloudWatch Alarm / Amazon SNS / AWS Chatbot などを利用できる。

併せて、EC2 インスタンスが稼働するハードウェアもしくはハイパーバイザーの障害でインスタンスが停止した場合、AutoRecovery の設定を行うことで復旧を自動化することができる。

ここまでの構成を図にまとめると以下のようになる。



5.2.11 AWS サービスでは提供されない機能

ここまでで説明したように、多くの要件は AWS サービスを活用することで充足することができる。ただし、以下の要件には対応できないため、必要に応じてサードパーティー製品・サービスを利用する必要がある。

- マルウェア対策
  - ユーザーがコンテンツをアップロードするようなワークロードでは対策することが望ましい
- IPS / IDS
  - IDS については、後述する Amazon GuardDuty で VPC Flow Logs を利用した脅威検知で一定の要件を満たすことが可能

5.2.12 Amazon RDS

ここまで、EC2 インスタンスの構成について述べたが、これらの対策と同等のことを Amazon RDS で実現する方法を本項で説明する。

結論としては、多くの機能が RDS の機能として自動化されている。具体的には、以下の機能は RDS インスタンスの作成時に設定するだけで利用できる。

- データベースのインストール
  - インストールおよび初期設定済みで、RDS インスタンス作成直後から利用可能
- 脆弱性管理
  - パッチがリリースされたら指定したメンテナンスウィンドウの範囲で自動適用
  - マイナーバージョンアップを自動的に実行しないことも可能
  - ただし、緊急度の高いセキュリティパッチは指定された期限までに強制的に適用されるため、それを前提として「どのように可用性を維持・運用するか」を検討しておく必要がある
- 暗号化
  - KMS と連携してボリュームの暗号化が可能
- ログ管理
  - CloudWatch Logs へエラーログや監査ログを配信可能
- バックアップ

- 指定したバックアップウィンドウの範囲で自動的にバックアップ
- 世代管理も自動化されている

- 監視
  - EC2 よりも詳細なメトリクスを標準で収集可能
  - フェールオーバーなどの RDS インスタンスで発生するイベントを Amazon SNS 経由で通知可能
    - ただし、AWS Chatbot には未対応
    - チャットサービスへ通知したい場合には AWS Lambda を利用する必要がある
- その他
  - Performance Insights による性能分析

このように、多くの運用管理タスクを RDS にオフロードすることができる。

5.3 AWS アカウント

本章の最後に AWS アカウント自体のセキュリティ対策について解説する。

5.3.1 認証・権限管理

AWS に作成する際の認証およびアクセス制御は AWS IAM（Identity and Access Management）を利用して管理することができる。

AWS アカウントを作成後、利用者を識別するための IAM User の作成や認証情報の設定を最初に実施するべきである。ちなみに、AWS アカウントのサインアップ時に利用できる Root ユーザーはあらゆる権限を有しており、なおかつ権限の制御もできないため、常用するべきではない。そのため、IAM User を作成する際には、最初に管理者権限を持つユーザーを作成し、以降の設定作業はこの管理者ユーザーで実行することが望ましい。なお、IAM User への権限付与は、IAM Group などを介して効率的に実施することが望ましい。また、適切な認証の強度を維持するためにパスワードポリシーや MFA を設定しましょう。

サインアップ直後は root アカウントしか存在しないが権限制御ができないため必要なとき以外は利用するべきではない。MFA を設定し、適切に管理することが推奨される。

また、AWS リソースへのアクセス許可は IAM のエンティティ（User・Role）への権限付与以外にリソースポリシーを利用することでも実現できる。このリソースポリシーによるアクセス許可は当該 AWS アカウント外の IAM エンティティに対しても権限を付与できる。そのため、意図しないアクセス許可による情報漏洩インシデントがしばしば発生している。Access Analyzer を利用することで、AWS アカウント外へのアクセス許可を検出および管理することができる。

5.3.2 証跡管理

AWS CloudTrail を利用して、AWS アカウント上で発生するほとんどのアクティビティのログを収集することができる。これにより、トラブルやインシデント発生時の調査などで活用できる。

ここで収集されたログは S3 に保存および CloudWatch Logs に配信することができ、Amazon Athena・CloudWatch Logs Insights などで分析することができる。併せて、CloudTrail Insights で、通常とは異なる頻度で発生した API 呼び出しを検知および分析することもできる。

このほか、ログファイルの整合性を検証できるオプションも提供されており、ログの完全性をより担保しやすくなっている。また、必要に応じて S3 オブジェクトの削除に MFA による認証を求めるような対策を追加することも可能である。

5.3.3 構成管理

AWS Config を利用して AWS リソースの構成変更を記録・管理することができる。AWS Config でサポートしている AWS リソースの構成や他のリソースとの関連を継続的に記録できるほか、Config Rules を利用することで AWS リソースの設定が指定した条件に反しているときに通知することもできる。これは後述するベースライン管理を実現するための前提となる。

EC2 を例に挙げて説明する。EC2 インスタンスは、作成から削除までのライフサイクルの間に起動や停止などの操作が行われる。また、時期によって負荷が高かったり低かったりする場合にはインスタンスタイプ（スペック）を変更することがある。このような変更を AWS Config を利用することで自動的に記録できる。また、EC2 インスタンス自体の記録だけでなく、どのリソースと関係性を持っているか、およびその関係性がどのように変化したのかも記録することができる。例えば、どの Security Group や EBS ボリュームが EC2 インスタンスに割り当てられているか、といった関係性を記録することができる。また、AWS Config は Security Group や EBS ボリュームなど多くのリソースの構成管理をサポートしている。

5.3.4 ベースライン管理

AWS を大規模かつ多様なサービスを活用して運用する時に課題となるのがベースライン管理である。例えば、Security Group で不必要なアクセス許可が設定されている／所定のストレージが暗号化されていない、などである。

Security Hub の Security Standard を利用することで、AWS アカウントに存在するリソースの設定にセキュリティリスクがないかを評価することができる。この機能を利用するためには、AWS Config と Security Hub が有効化されていることが前提となる。

Security Hub の Security Standard では、「PCI DSS」「AWS Security Best Practice」「CIS Benchmark」などに準拠したルールを利用できる。

また、Trusted Advisor を利用することでセキュリティ以外の観点でも AWS アカウントの状態を確認することができ、AWS アカウント内で作成したリソース数が上限に近づいていないか、などを確認できる。

5.3.5コスト管理

AWS は従量課金のため、適切なコスト管理が非常に重要である。具体的には、以下のような対策を実施することが望ましい。

- 利用料金が予算を超過しないように監視する
- 利用明細を分析し、不要な支出を削減する（利用費の上位を占める科目を特定し、削減の余地がないか確認する）
- システムの特性に応じてオンデマンド以外の購入オプションを検討する
- リソースを占有するタイプのサービスを利用している場合、適切なサイズに変更する

料金の監視には AWS Budgets が利用できる。指定した閾値に到達したもしくは到達する可能性がある場合にシステム管理者へ通知を行うことができる。なお、Budgets からの通知は AWS Chatbot での通知をサポートしている。

また AWS の料金の分析には Cost Explorer を利用して利用料金を分析することができる。具体的には、「月・日単位の料金推移をグラフ化」「サービス別に料金推移をグルーピング」「特定の科目のみを表示するようにフィルタリング」などを行うことができる。

AWS リソースが年単位で 24 時間稼働する場合、リザーブドインスタンスもしくは Savings Plans を購入することで大幅なディスカウントを適用することができる。具体的にどの程度のディスカウントが可能かは Cot Explorer 内の推奨事項で確認できる。

また、リソースの利用率に基づいて EC2 インスタンスの適切なサイズを推奨する機能も Cost Explorer から提供されている。

5.3.6脅威検知および分析

AWS アカウントおよびそこで作成されたリソースは常に第三者による不正のリスクに晒されている。もし不正が発生した場合にはしかるべき対応を実施する必要があるが、そもそも不正に気づくこと自体が一般的には困難である。例えば、「ワークロード上のアクティビティがどのに・どのように記録されるのかを把握（監視対象の特定）」「どのようなアクティビティを不正と判断するのかを定義（ルールの定義）」「不正アクセスに

関するトレンドや Malicious IP 等の情報収集」などを一般的な組織が単独で行うことは困難である。そのため、一般的にはセキュリティベンダーの提供するセキュリティソリューションを利用することでこのような課題の解決を図る。

Amazon GuardDuty を利用することで、CloudTrail / VPC Flow Logs / DNS Query Logs に基づいてセキュリティリスクのあるアクティビティを検知することができる。

また、Detective を事前に有効化しておくことで、検知された脅威を起点に各種ログの追跡を行うことができる。その他にも、SIEM としての Amazon Elasticsearch Service やサードパーティーのサービスを利用することもできる。

5.3.7 イベント対応

AWS アカウントを運用管理していると、AWS に起因する様々なイベントが発生する。

具体的には以下のようなものがある。

- AWS 自体の障害
- メンテナンスイベント
- Abuse（不正利用）
- ソフトウェアのサポートライフサイクルに起因するイベント（EOL に達したソフトウェアに依存するリソースの提供終了など）

AWS Health（Personal Health Dashboard）を利用することで、AWS の利用者がこれらのイベントの発生を認識することができ、意図しないサービスの停止などを回避することができる。

AWS Health は Event Bridge を介してイベントの発生をトリガに通知などを行うことができる。

5.3.8AWS サポートの利用

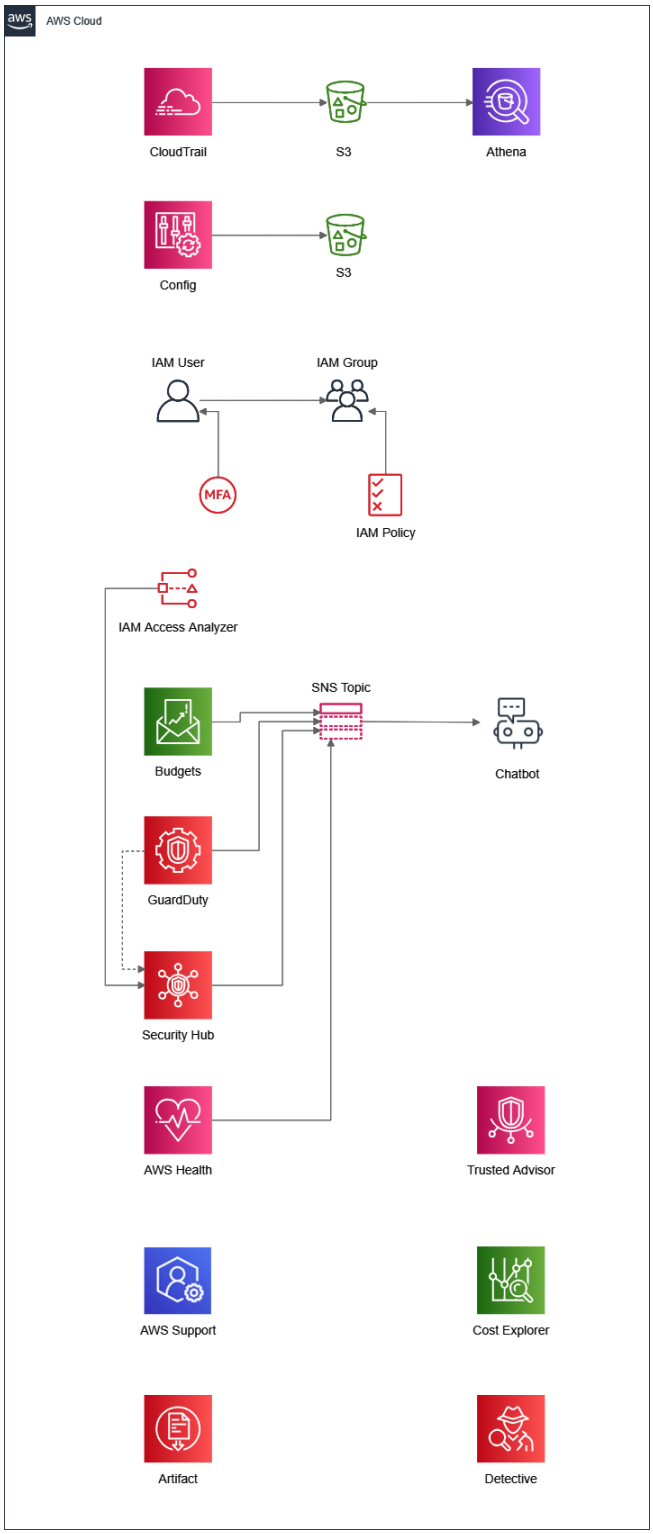
AWS 利用する中で発生する障害に対応するために、AWS の技術支援を必要とする場合がある。

AWS サポートを利用することでプランに応じたサービスレベルの技術支援を受けることができる。

5.3.9準拠法・管轄裁判所

AWS をサインアップする際、AWS の定める AWS カスタマーアグリーメント（利用規約）に同意する必要がある。例えば、AWS カスタマーアグリーメントでは、「AWS と AWS の利用者との間で紛争になったときにどの裁判所で争うのか（管轄裁判所）」「契約の有効性や解釈をどこの法律に基づいて判断するのか（準拠法）」「AWS を利用することで発生した損害に対する賠償責任の有無もしくはその上限」などを定めています。既定の AWS カスタマーアグリーメントでは、準拠法および管轄裁判所が米国のものとなっている。

AWS Artifact を利用することで、これを日本法／東京地方裁判所に変更することができる。


AWS Cloud
CloudTrail
S3
Athena
Config
S3
IAM User
IAM Group
MFA
IAM Policy
IAM Access Analyzer
SNS Topic
Budgets
Chatbot
GuardDuty
Security Hub
AWS Health
Trusted Advisor
AWS Support
Cost Explorer
Artifact
Detective

本ドキュメントの利用については、付属の『ASCJ クラウドセキュリティガイダンス＆ベストプラクティス利用許諾規約』に同意したものとみなす。

注 1）

https://www.wired.com/story/billion-records-exposed-online/

https://www.comparitech.com/blog/information-security/2-7-billion-email-addresses-exposed-online/

https://www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident/

https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/

注 2）

政府機関等の情報セキュリティ対策のための統一基準

https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf

注 3）

経済産業省情報セキュリティ管理規程

https://www.meti.go.jp/intro/data/pdf/kanri_kitei.pdf

注 4）

経済産業省情報セキュリティ対策基準

https://www.meti.go.jp/intro/data/pdf/taisaku_kijun_1906.pdf

注 5）

政府情報システムのためのセキュリティ評価制度（ISMAP）

https://www.ipa.go.jp/security/ismap/index.html

注 6）

欧州ネットワーク情報セキュリティ庁（ENISA）

https://www.enisa.europa.eu/

注 7）

Cloud Control Matrix（CCM）

https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/

注 8）

FISC 安全対策基準

https://www.fisc.or.jp/publication/guideline.php

注 9）

3 省 3 ガイドライン

①厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版」

https://www.mhlw.go.jp/stf/shingi2/0000166275.html

②総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」

http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000209.html

③経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン　第2版」

https://www.meti.go.jp/policy/it_policy/privacy/iryouglv2.pdf

注 10）

世界 IaaS パブリッククラウド市場は 31%成長、AWS がシェア約 5 割--ガートナー

https://japan.zdnet.com/article/35140599/

注 11）

https://d1.awsstatic.com/whitepapers/ja_JP/aws_cloud_adoption_framework.pdf

注 12）

https://docs.aws.amazon.com

注 13）

PCI DSS（Payment Card Industry Data Security Standard）とは、カード会員情報の保護を目的として、国際ペイメントブランド 5 社が共同で策定したカード情報セキュリティの国際統一基準

https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

<u>参考資料</u>

1. セキュリティで推進するクラウドジャーニー　～セキュリティ上の論点と打ち手～
https://pages.awscloud.com/rs/112-TZM-766/images/AWSTransformationDayTokyo_AWS_Security_CloudJ_handsout.pdf

2.クラウドジャーニーの現在

https://pages.awscloud.com/rs/112-TZM-766/images/H-01.pdf

3.クラウドジャーニー事例の活用ススメ

https://dev.classmethod.jp/articles/usage-aws-cloud-journey/

4.AWS Cloud Adoption Framework

https://aws.amazon.com/jp/professional-services/CAF/

5.AWS Cloud Adoption Framework で作成するクラウド導入ロードマップ

https://d1.awsstatic.com/events/jp/2017/summit/slide/D4T1-1.pdf

6.責任共有モデル

https://aws.amazon.com/jp/compliance/shared-responsibility-model/

7.責任共有モデルとは何か、を改めて考える

https://aws.amazon.com/jp/blogs/news/rethinksharedresponsibility/

8.【AWS セキュリティ入門】徒然なるままに責任共有モデルの下から上までそこはかとなく解説

https://jpn.nec.com/cloud/service/aws/pdf/JAWS_DAYS_2019_NEC-AWS_security_20190223.pdf

9.AWS のデータセンター

https://aws.amazon.com/jp/compliance/data-center/data-centers/

10.AWS のコントロール

https://aws.amazon.com/jp/compliance/data-center/controls/

11.データプライバシー

https://aws.amazon.com/jp/compliance/data-privacy-faq/

12.コンプライアンスリソース

https://aws.amazon.com/jp/compliance/resources/

13.AWS コンプライアンスプログラム

https://aws.amazon.com/jp/compliance/programs/

14.コンプライアンスプログラムによる AWS 対象範囲内のサービス

https://aws.amazon.com/jp/compliance/services-in-scope/

15.AWS の製品・サービス一覧

https://aws.amazon.com/jp/products/

16.AWS:セキュリティプロセスの概要

https://aws.amazon.com/jp/whitepapers/overview-of-security-processes/

改版履歴

版数	日付	改版内容
1.0	2020 年 12 月 8 日	