salesforce app cloud

Salesforce Heroku Enterprise

クラウドセキュリティの概要

目次

はじめに

Heroku EnterpriseはSalesforce App Cloudファミリーの根幹をなす製品であり、クラウド型アプリケーションプラットフォームとして、世界中のあらゆる規模の企業がアプリケーションを展開、運用する基盤として採用しています。Herokuはクラウド黎明期に、最も早い時期から提供が始まったPaaSの1つで、Herokuを導入した企業は、インフラストラクチャの管理や拡張、セキュリティの確保をSalesforceとHerokuに任せることで、アプリケーション開発およびビジネス戦略に専念しています。

つまり、Herokuが各種セキュリティベストプラクティスを実施し、プラットフォームのセキュリティを管理するため、利用者は自社のビジネスにのみ集中できるのです。Herokuでは物理層からアプリケーション層まで、すべてのレイヤーのセキュリティを管理することで、お客様を脅威から守ります。アプリケーションとデータが分離されているため、お客様の手をわずらわせることなくセキュリティプログラムの更新が行われ、サービスが中断されることもありません。

エンタープライズクラスの開発環境を提供するHeroku Enterpriseは、以下を実現します。

- **コラボレーション**
  チームでアプリケーションを開発するための共有ワークスペースを提供
- **信頼性**
  強化されたサポートSLAとソリューションアーキテクチャチームにより、トラフィック急増時の対応、アプリケーションアーキテクチャの設計、オンボーディングをきめ細かくサポート
- **可視性**
  アプリケーションポートフォリオ全体の状況を把握し、リソースの管理と使用量を最適化
- **アクセス制御**
  シームレスに連携する権限セットにより、開発者や管理者に必要なアクセス権をすばやく付与

Salesforceのトラストモデル

お客様の情報の機密性、完全性、可用性は、お客様のビジネスの成功にとって不可欠です。そして、お客様の成功こそがSalesforceの目指すものです。Salesforceでは、多層的アプローチで重要な情報を保護し、増え続けるセキュリティへの要求と課題に対応するため、常にアプリケーション、システム、プロセスを監視、改良しています。

セキュリティに対する責任と意識は、社内のあらゆるレベルで共有されています。SalesforceとHerokuのいずれにとっても、お客様データの保護がサービス提供の基本原則です。Salesforceでは、多くの組織、チーム、個人がセキュリティに関連する業務を担当しています。チーフトラストオフィサーは情報、製品、企業セキュリティ、エンタープライズリスク管理、技術監査、コンプライアンスを含むSalesforceのセキュリティプログラムと担当者を監督します。また、グローバルプライバシーカウンシルは、Salesforceのプライバシープログラムを管理し、各国の個人情報保護法やデータ保護法への対応などを行っています。さらに、すべての従業員は機密保持、プライバシー、情報セキュリティの規定に従うことが義務付けられています。

> 詳細については、以下のリンク先をご参照ください。
> **trust.salesforce.com/trust/jp/**
> **heroku.com/policy/security（英語）**

クラウドコンピューティングの責任共有モデル

米国国立標準技術研究所（NIST）はクラウドコンピューティングを「動的に構成可能な共有のコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続き、またはサービスプロバイダとのやりとりで速やかに割当てられ、提供されるものである」と定義しています。標準的なサービスモデルとしては、SaaS（サービスとしてのソフトウェア）、PaaS（サービスとしてのプラットフォーム）、IaaS（サービスとしてのインフラストラクチャ）の3種類があります。SalesforceはSaaSのプロバイダーと思われがちですが、App CloudとHeroku EnterpriseはPaaS製品です。

PaaS製品では、サービスを提供する事業者（Salesforce）とサービスの利用者の双方がセキュリティとコンプライアンスの実現に向けて取り組むことが求められます。以下の図に、事業者と利用者（テナント）がそれぞれに負うべき責任を示します。

	IaaS	PaaS	SaaS
アプリケーション	テナント	テナント	事業者
データ	テナント	双方	事業者
ランタイム	テナント	事業者	事業者
ミドルウェア	テナント	事業者	事業者
OS	テナント	事業者	事業者
仮想化	事業者	事業者	事業者
サーバー	事業者	事業者	事業者
ストレージ	事業者	事業者	事業者
ネットワーク	事業者	事業者	事業者

Salesforceは、クラウドアプリケーションとデータサービスのプラットフォームであるHerokuを、サードパーティのインフラストラクチャプロバイダーであるAmazonでホストしています。Herokuの基盤インフラストラクチャ層の一部にはアマゾンウェブサービス（AWS）を活用しています。この構成では、Herokuが提供する機能の一部にAWSの機能が利用されていますが、サービス提供事業者としての全責任はHerokuが負っています。

事業者側の責任範囲

サービスを提供する側として、Herokuは以下に挙げる項目に関して主要な管理業務を担い、サービス実現に努めています。

インフラストラクチャとアプリケーションのセキュリティ – Herokuは基盤となるコンピューティングサービスのうち設計、デプロイ、保守を行うほか、セキュリティ対策の責任を負います。その対象には、テナントのランタイムを支える仮想マシンとアプリケーションマイクロサービスが含まれます。また、お客様の代わりにHerokuが独占的管理アクセス権を有する要素に対しても、Herokuが責任を負います。

セキュリティの監視 – Herokuが独占的管理権限を有するインフラストラクチャサービスとプラットフォームサービスに関し、各種のツールとポリシーを活用して包括的なセキュリティ監視とイベントログの記録を実施します。

パッチ管理 – Herokuは、クラウドアプリケーションプラットフォームを提供するために使用するオペレーティングシステムとアプリケーションの保守を行います。これには、システムとアプリケーションに不可欠とみなされるパッチの適用が含まれます。

ネットワークセキュリティ – お客様のアプリケーションを実行する情報システムを含むネットワークについては、Herokuが保護します。お客様が直接管理するアプリケーション環境のアクセスレベル、統制、構成に関しては、お客様が責任を負います。

物理セキュリティ – 物理データセンターについては、Herokuが物理面と環境面の両方の統制に保護責任を負います。対象となるデータセンターには、Herokuが直接運営する施設と、IaaSの運営に利用するサードパーティのクラウドプロバイダーの施設の両方が含まれます。

テナント側の責任範囲

テナントアプリケーションのセキュリティを徹底するためには、テナントとしてHerokuプラットフォームを使用するお客様も重要な責務を担います。

- **アプリケーション設計** – テナントは、Heroku上で実行するアプリケーションの安全性を確保して設計するという責任を負います。これには、データへのアクセスと該当するアプリケーションによって制御されるシステム構成も含まれます。具体的には、適切なIDアクセス制御と管理、TLS終端にとどまらないエンドツーエンドの暗号化、セキュリティ対策およびHerokuから提供された証明書の保管、アプリケーションのエンドユーザーに付与されるロールとアクセス権限の割り当てが含まれますが、これらに限定されません。

- **セキュリティの監視** – テナントが構成して管理するアプリケーション環境やデータベース環境内で発生する、すべてのセキュリティイベントの検知、分類、改善については、テナントが責任を負います。Herokuが管理するインフラストラクチャやサービスで保証されていない、テナントが参加しているコンプライアンスプログラムまたは認定プログラムに関連した監視に関しても、テナントが責任を負います。ただし、Heroku PostgresやHeroku Redisといった、Herokuが管理するデータサービスのセキュリティ監視については、Herokuが実施します。

> "パッチの適用も、ストレージの追加も、セキュリティの脆弱性も心配する必要はありません。Herokuプラットフォームの管理とサポートは、Herokuチームに任せています。"
>
> Align Technology社
> ドクターポータルおよびビジネスサポート部門、シニアマネージャー
> **LEELA PARVATHANENI氏**

インフラストラクチャとアプリケーションのセキュリティ

サーバーの強化

HerokuはOSイメージ（スタック）を強化するため、デフォルトですべてのサービスとコンポーネントを無効にしています。業務上や運用上の正当な目的がある場合にのみ、個別に有効化できます。

テナントのアプリケーション

Herokuプラットフォーム上の各アプリケーションは隔離された専用の環境内で実行され、ほかのアプリケーションやシステム内の別の領域とは通信できません。運用環境にこうした制限を設けているのは、セキュリティと安定性に問題が発生するのを避けるためです。この自己完結型の環境では、Linuxコンテナ（LXC）を使用してプロセス、メモリ、ファイルシステムを分離すると同時に、ホストベースのファイアウォールによってアプリケーションのローカルネットワーク接続の確立を制限しています。

> 技術情報の詳細については、以下のリンク先をご参照ください。
> **devcenter.heroku.com/articles/dyno-isolation（英語）**

Dynoコンテナの強化

Herokuのカーネル内では、カーネルのバグによってホストに脆弱性が生まれないよう、リスクの予防策が複数実行されます。まず、Herokuはセキュアコンピューティングモード（seccomp）を使用してシステムコールをフィルタリングします。seccompはLinuxカーネル内でアプリケーションをサンドボックス化するためのセキュリティ機構です。また、コンテナ内ではroot権限が明示的に拒否されるように構成されており、ファイルシステムのマウントやカーネルモジュールのロードといった一部の機能は、コンテナ内では実行が中止されます。

HerokuのCommon Runtime環境とPrivate Spaces Runtime環境には、いくつか相違点があります。Heroku Common Runtimeは、マルチテナントとシングルテナントの両方のアーキテクチャ特性を備え、コンテナではAppArmorが利用されます。AppArmorとは、Linux Security Moduleを使用してプログラムを制限し、Linuxのサービスを保護する強制アクセス制御（MAC）システムです。一方、Heroku Private Spaces Runtimeではテナント間を完全に切り離し、コンピューティングインスタンスごとに1つのコンテナを割り当てて、実行環境全体をそれぞれの専用インスタンス上で運用します。

アプリケーションのセキュリティ

Herokuでは、広範な侵入テスト、脆弱性の評価、ソースコードのレビューを社内で実施し、アプリケーションやアーキテクチャのセキュリティを評価しています。また、OWASP Top 10に挙げられているWebアプリケーションの脆弱性チェックやアプリケーションの分離といった、外部のセキュリティ評価基準をHerokuプラットフォーム全体に採り入れています。Herokuは外部のセキュリティ評価機関と緊密に連携してプラットフォームやアプリケーションのセキュリティを点検し、各種のベストプラクティスを適用しています。

Herokuはさまざまなソースから脆弱性データを入手し、脆弱性を検出してパッチを適用しています。たとえば、仮想侵入者チームは定期的な監査を行い、外部機関や内部で侵入テストを実施しています。また、バグ懸賞金プログラム（bugcrowd.com/heroku）を展開し、オープンソースコミュニティで脆弱性データも収集しています。さらに、こうしたプログラムを補完するため、内部と外部でセキュリティスキャンも実施しています。

Herokuアプリケーションに問題が見つかった場合は、リスクレベルを評価して優先度を設定し、対応チームに割り当てて問題の改善を図ります。さらに、Herokuのセキュリティチームが改善プランをつぶさに確認し、適切な解決策を実施します。

> お客様自身でHeroku上にあるアプリケーションのセキュリティスキャンを実施することもできますが、外部のテストを実施する場合は、あらかじめHerokuにご連絡ください。
> **devcenter.heroku.com/articles/pentest-instructions（英語）**

Herokuは常にセキュアな開発ライフサイクルを実践しています。Herokuのセキュリティチームはエンジニアリングチームと緊密に連携しながらアーキテクチャやコードを見直し、安全性のリスクが高いすべての機能に対して、侵入テストを実施しています。四半期ごとの製品計画にはセキュリティチームも参加して、新機能の開発に伴い、セキュリティ上の影響がないかを確認し、リスクの高いプロジェクトを特定します。リスクが高いと判断されたプロジェクトは、セキュリティチームのレビュー対象となります。このプロセスでは、初期段階でのセキュリティ評価、安全性の高いコーディングに関するガイドラインの周知徹底、仮想侵入者チームによる定期的な監査のほか、社内外での侵入テストも行われ、そのすべてをセキュリティチームが実施し、監督します。

Herokuでは、プラットフォームのインテグレーションテストサービスを活用し、外部のHerokuユーザーの観点からエンドツーエンドのテストを実施して、ユーザー向けに機能を提供する際に必要となるさまざまなサービスをテストしています。このサービスでは、単発のテストと監視を目的とした継続的なテストを両方実施します。そのほかに、Herokuはサードパーティ製のテストツールを使用して、プラットフォームのソフトウェアコンポーネントをリポジトリレベルでテストしています。

Heroku Flow

Heroku Flowは、アプリケーションの開発プロセスを合理化する継続的デリバリー（CD）を行うためのツールセットです。Heroku Pipelineを活用することで、ステージ間でのコードの移動を自動的に行えます。パイプラインとは、同じコードベースを共有するHerokuアプリケーションのグループです。パイプライン内のアプリケーションは、継続的デリバリーフローでデプロイされる、レビュー、開発、ステージング、本番という4種類のステージのいずれかに登録されています。豊富な管理統制機能を使って、Heroku Pipelineで管理するソフトウェアをステージごとに制御できます。アプリケーションにはそれぞれ、管理、デプロイ、運用の権限があるユーザーからなる、固有のグループを割り当てることができます。この機能を活用すれば、レビューステージと開発ステージでは幅広いユーザーによるコラボレーションが可能になり、一方でステージング環境と本番環境に昇格されたアプリケーションについては、ガバナンスと統制を強化できます。

IDとアクセスの管理

アカウントの種類

Herokuプラットフォームへのアクセスに使用するアカウントは2種類あります。

- **Herokuアプリケーションアカウント** – Herokuのお客様であるユーザー（主にソフトウェア開発者）がアプリケーションの管理を行うのに使用します。
- **プラットフォーム管理アカウント** – プラットフォームの運用に携わるHerokuの社員が使用します。システムの運用と管理を行うため、上位の権限が与えられます。

しかしながら、プラットフォームはほとんどがHerokuアプリケーションで構成されているため、Herokuの管理者は常にアプリケーションアカウントとプラットフォーム管理アカウントの両方を使用して日常的な管理タスクを実行します。

Herokuアプリケーションアカウントにログインするには、アルファベット、数字、記号を組み合わせた8文字以上のパスワードを設定します。プラットフォーム管理アカウントは、承認済みのHeroku運営スタッフのみに付与され、セキュリティチームが職責にもとづいて一元管理します。プラットフォーム管理アカウントには、必要に応じて上位の権限が割り当てられ、Herokuプラットフォーム内のプラットフォームシステムを管理できます。Herokuプラットフォームへのアクセスには、2要素認証が必須です。

salesforce app cloud

IDとアクセスの管理（続き）

SalesforceのIT部門は、すべてのワークステーションへのアクセスを管理し、すべての社員にネットワークパスワードを90日ごとに変更するよう義務付けています。また、全社的なパスワードポリシーとして、以下が定められています。

- **最低文字数** – 15文字
- **文字種** – 大文字の英字、小文字の英字、数字、記号、絵文字を使用可（この中から少なくとも3種類を混ぜて使用）
- **多要素認証**

パスワードはまったく違ったものに変更する必要があります。一度使用したパスワードを再利用することはできません。パスワードへの総当たり攻撃や盗難、共有を避けるため、オペレーティングシステムではパスワード認証を使用できません。Heroku管理者がシステムをリモート操作する際は、セキュアなSSH接続を使用しています。

シングルサインオンによるIDの連携

Herokuはユーザーの既存のIDプロバイダー（IdP）と簡単に連携できるため、ほかのサービスプロバイダーと同じログイン情報とログイン方法を使用する、シングルサインオン（SSO）でHerokuにアクセスできます。HerokuのSSO機能は、SAML 2.0に対応しています。
Herokuでは、以下に挙げるIDプロバイダーを標準でサポートしています。

- Auth0
- Azure Active Directory
- Bitium
- Okta
- PingFederate
- Ping Identity
- Salesforce Identity

組織、ロール、アクセス権限

現在、Heroku Enterpriseでのみ利用可能な組織アカウントでは、Herokuアプリケーションを企業、あるいはその他のグループとして管理できます。組織アカウントを使用すると、一連のアプリケーションが共有のコレクションとして扱われ、コレクション内にある各アプリケーションへの特定のアクセス権を開発者グループに割り当て、組織全体のリソース使用状況を監視できます。

組織内のユーザーには、管理者ロールまたはメンバーロールのどちらかを割り当てることができます。それぞれのロールの数に制限はありませんが、各組織に少なくとも1名の管理者ユーザーが必要です。組織のメンバーには、メンバーロールに加えて、組織が所有する特定のアプリケーションに対するアプリケーション権限を割り当てることも可能です。

管理者

管理者ロールでは、以下のことを行えます。

- 組織内の管理者とメンバーを追加、削除
- 組織内外のユーザーにアプリケーションの各種権限を付与
- リソースを確認して組織の請求情報にアクセス
- 組織内の全アプリケーションを表示してアクセス（ロックされたものを含む）
- 組織内のアプリケーションを操作（デプロイ、Dynoの拡張、アドオンの管理、削除など）
- アプリケーションを組織内外に転送

各組織には最低1名の管理者ユーザーが必要です。そのため、組織内の管理者が1名のみの場合、その管理者を削除することはできません。また、管理者ユーザーを追加できるのは、別の管理者のみです。

組織、ロール、アクセス権限（続き）

メンバー

メンバーロールを割り当てられたユーザーは、組織内の全アプリケーションに読み取り専用でアクセスできます。メンバーユーザーを追加できるのは組織の管理者ユーザーのみです。メンバーロールでは、以下のことを行えます。

- 組織内の全アプリケーションを表示
- ロックされていないアプリケーションにアクセスして基本情報を確認（誰がどのような権限を持っているかなど）
- 特定のアプリケーションをデプロイ、運用、管理（権限を付与された場合）
- 組織内でアプリケーションを作成
- 個人用アプリケーションを組織に転送
- 自身が作成または転送したアプリケーションを操作
- 組織内のリソース、管理者、メンバーを確認

メンバー以外

組織の正式なメンバーではないユーザーには、アプリケーションレベルの権限を付与すると、特定のアプリケーションにのみアクセスできるようになります。アプリケーションレベルの権限は、アプリケーションの管理権限を持つ組織管理者またはメンバーが、任意の権限を組み合わせて付与することができます。この権限を与えられると、以下のことを行えます。

- 別の組織アプリケーションへのアクセス権を表示
- 別の組織ユーザーを表示
- アプリケーションを作成、または組織に転送

ネットワークセキュリティ

セキュアなネットワークアーキテクチャ

ネットワークの外部との境界、およびネットワーク内の主要な内部境界には、各種ネットワークデバイス（ファイアウォールをはじめとする境界デバイスなど）を設置して通信の監視と制御を行っています。デフォルトではすべてのアクセスが拒否され、ビジネスニーズにもとづいて明示的に許可されたポートとプロトコルのみが有効化されます。各システムには、それぞれの機能に応じてファイアウォールのセキュリティグループが割り当てられます。セキュリティグループは、システムの特定の機能に必要なポートとプロトコルのみにアクセスできるよう制限することでリスクを軽減します。

ホストベースのファイアウォールは、ループバックネットワークインターフェースを介して、ユーザーのアプリケーションがローカルホスト接続を確立するのを防止し、アプリケーションを確実に分離します。ホストベースのファイアウォールは、必要に応じてインバウンドとアウトバウンドの接続をさらに制限します。

セキュアなアクセスポイント

Herokuのデータセンタープロバイダーは、クラウドサービスへのアクセスポイントの数を制限して、インバウンド通信やアウトバウンド通信、ネットワークトラフィックの監視を強化しています。ユーザー用のアクセスポイントは、セキュアなHTTPアクセス（HTTPS）をサポートしているため、Herokuのランタイムとの間にセキュアな通信セッションを確立できます。

さらに、Herokuのデータセンタープロバイダーは、インターネットサービスプロバイダー（ISP）との接続専用のネットワークデバイスを備えています。このプロバイダーのデータセンターでは、インターネットとの接点となるデータセンターネットワークの各エッジにおいて、複数の通信サービスに対する接続を冗長化しています。こうした接続には、それぞれに専用のネットワークデバイスが配置されています。

転送中のデータ

インスタンス間で転送中のデータはすべて、SSL（TLS）を通じてデフォルトで暗号化されます。つまり、シングルテナントDynoとPrivate Spaces Runtime間のトラフィックはすべて暗号化されますが、同一インスタンス内で実行されるマルチテナントDyno間の通信は暗号化されない場合があります。暗号化アルゴリズムはブラウザーとエンドポイントとのネゴシエーションで決定されます。インターネットトラフィックはすべて、デフォルトで暗号化されます。

salesforce app cloud

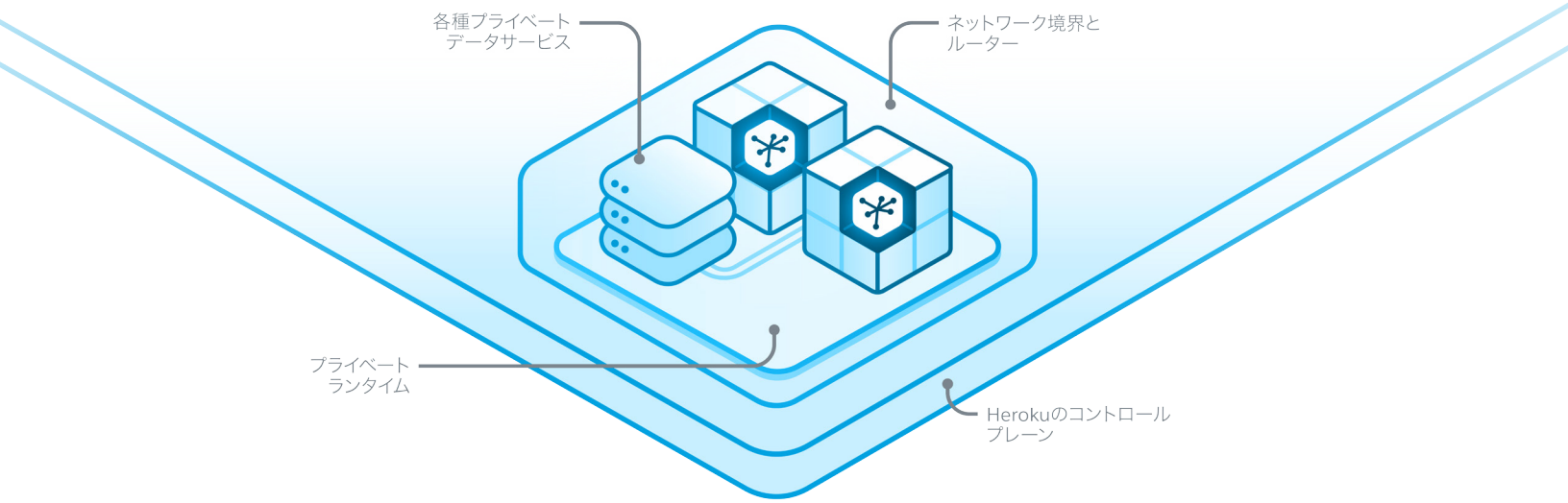
Private Spaces

ネットワークセキュリティをさらに強化したい場合には、Heroku Private Spacesを活用できます。Private Spacesは、Heroku上で一連のアプリケーションやデータサービスと専用のランタイム環境からなる隔離されたネットワーク環境を提供するもので、プロビジョニングするリージョンを指定できます。Private Spacesを使用すると、Herokuの強力な開発環境を使用して最新のアプリケーションを作成できるうえ、エンタープライズレベルのセキュアなネットワークトポロジーが形成されて、オンプレミスのシステムやほかのクラウドサービスに安全に接続できます。

Private Spacesの作成、破棄、設定変更といった管理機能は、組織の管理者のみが実行できます。それぞれの非公開スペースには、信頼できるIPアドレス範囲のセットが割り当てられており、非公開スペース内で実行されるWebプロセスには、このIPアドレス範囲のいずれかと合致するクライアントしかアクセスできません。非公開スペース内にあるアプリケーションからのアウトバウンドトラフィックは、すべてそのスペース専用の、永続的に割り当てられた少数のIPアドレスから発信されます。そのため、IPのホワイトリスト機能を使用して、スペース内にあるアプリケーションがアクセスするサービスのセキュリティを確保できます。

Heroku PostgresやHeroku RedisといったHerokuのデータサービスは、Heroku Private Spaces内に作成されます。こうしたデータサービスは、自動的にHeroku Private Spacesと同じリージョン内に作成され、Heroku Private Spacesと対応付けられます。

Heroku Private Spaces



詳細については、以下のリンク先をご参照ください。
heroku.com/private-spaces（英語）

データセキュリティ

Heroku Postgres

ユーザーのデータは、アクセス制限されて物理的に隔離されたデータベースに格納されます。各データベースにアクセスするには、特定のデータベースでのみ有効で、かつアプリケーション固有である一意のユーザー名とパスワードが必要です。複数のアプリケーションとデータベースを保有する場合は、不正アクセスのリスクを軽減するため、それぞれに別のデータベースインスタンスとアカウントが割り当てられます。

Postgresデータベースにアクセスする際は、SSL暗号化を使用し、高度なセキュリティとプライバシーを確保する必要があります。また、アプリケーションをデプロイする場合は、暗号化してデータベースに接続することを推奨しています。

格納されたデータは、データのセキュリティ要件に応じてユーザーのアプリケーションで暗号化できます。また、アプリケーションをデプロイする際には、データストレージ、鍵の管理、データ保持の要件を組み込むことができます。

暗号化

Heroku PostgresデータベースのPremiumプランとEnterpriseプランでは、ブロックレベルのストレージ暗号化方式であるAES-256を使用して保管中のデータを暗号化します。データの暗号化は、AWSのEBSディスク暗号化機能を使用して実装されています。暗号化鍵はすべてAWSで管理され、Herokuの担当者も、もちろんほかのお客様も見ることはできません。Postgresにアクセスするためのログイン情報も、暗号化されて保管されます。

データの保持と破棄

アプリケーションによって格納されるデータはHerokuのユーザーが定義します。また、データ保持要件に沿ってデータベースからデータを消去することについては、ユーザーが責任を負います。ユーザーがアプリケーションや関連するデータベースのプロビジョニングを解除した場合、Herokuはそのデータベースのストレージボリュームを少なくとも1週間維持します。その期間が過ぎると自動的にボリュームが破棄され、データを復旧できなくなります。物理ストレージボリュームのプロビジョニング解除については、「物理セキュリティ」の項で説明します。

セキュリティの監視

ログの記録とネットワークの監視

Herokuのセキュリティ担当とエンジニアリング担当のスタッフは、さまざまなツールとログフィードを監視して、異常な動作がないかチェックしています。こうしたチームで、認証イベント、sudoのリクエスト、データトラフィックのパターンなどの各種データソースを確認します。

ネットワークに関しては、Herokuはアクセスログを収集して不正利用や不適切なアクセスがないか継続的に点検しています。また、インフラストラクチャプロバイダーであるAWSからも、不正利用に関するデータを受け取ります。

Herokuのログ収集はLogplexを基盤としています。Logplexは複数のソースからログを集め、「ドレイン」と呼ばれる最終的な宛先に集約します。Herokuでは、ログの集約や分析用のツールを実行するシングルテナントインスタンスがホストされます。セキュリティログは、適切な権限を持つHerokuの担当者しか見ることができません。

DDoS

Herokuプラットフォームは、TCP SYN Cookieや接続速度の制限などでネットワーク層でのDDoS攻撃を防いでいます。Herokuプラットフォームでは複数のバックボーン接続を用意し、インターネットキャリアから提供される帯域幅以上の帯域容量を内部で確保しています。Herokuはネットワークプロバイダーと密接に連携し、必要になれば即座にイベントに対応してDDoS対策を実行できるよう備えています。

アプリケーション層でもDDoS対策が必要であれば、テナントレベルで攻撃の緩和策を講じます。DDoS攻撃への不安がある場合、以下に挙げる対策のどちらか、または両方を実施するようお勧めします。

- DDoS対策機能を持つコンテンツデリバリーネットワーク（CDN）機能を、ユーザーのアプリケーションの前方に配置します。CloudFlareがよく使用されます。
- 各アプリケーションフレームワークに応じたプラグインで、アプリケーション層での速度制限やブロックを行えます。使用できるツールは、採用している言語とフレームワークによって異なりますが、たとえば、Rack::Attack（Ruby）、turnstile（Python）、node-rate-limiter（Node.js）などがあります。

中間者攻撃とIPスプーフィング

マネージドファイアウォールを使用すると、ネットワーク上、あるいは仮想ホスト間でのIP、MAC、ARPのスプーフィングを防ぎ、スプーフィングの実行が不可能になります。また、ハイパーバイザーなどのインフラストラクチャがパケット盗聴を防止するため、宛先アドレス以外のインターフェースにトラフィックが送信されることはありません。Herokuはアプリケーションの分離、オペレーティングシステムの制限、暗号化接続などを採り入れ、あらゆるレベルでリスクを軽減するよう努めています。

パッチ管理

Herokuはプラットフォームを常にアップグレードして改良していますが、この作業がアプリケーションの実行に影響することは通常ありません。緊急性が低く、ダウンタイムを要するパッチについては、ユーザーが自分の都合にあわせてメンテナンスウィンドウを設定し、アップグレードを実行できます。OS関連のパッチは、ユーザーに影響を与えることなくすみやかに適用されます。脆弱性を管理するプロセスは、極力お客様に手間をかけることのないよう、また影響を及ぼすことなくリスクを修正できるよう設計されています。

脆弱性への対応はHerokuのセキュリティチームが担当しています。脅威情報は各種の内部ツール、エンジニアリングチームと運用チーム、セキュリティチームによる調査のほか、公開ソースから手に入る脆弱性情報や、Herokuのバグ懸賞金プログラムのような外部プログラムを通じて収集しています。脆弱性情報は一つひとつ検討し、Heroku環境に当てはまるか判断して、リスクに応じてランク分けした後、適切なチームに割り当てて解決を図ります。脆弱性のリスクレベルは4段階に分類され、「重大」は7日以内、「高」は30日以内、「中」は60日以内、「低」は90日以内にパッチを適用します。

パッチに関する通知

Herokuでは継続的に、また必要に応じてパッチを適用しています。通常、重要度の低いパッチについてはユーザーに通知しませんが、比較的重要度の高いリリースについてはHerokuの変更ログに通知します。データベースのアップグレードによってダウンタイムの発生が予想される場合など、ユーザーに直接影響を及ぼすパッチについては、事前にユーザーに通知し、メンテナンスウィンドウを設定します。

> こうした変更については、Herokuのステータスサイトでもお知らせしています。
> **status.heroku.com（英語）**

セキュリティ対応事例 – glibcの場合(1)

HerokuによるglibcのBeyaku性への対応

2016年2月、Googleのセキュリティ部門とRed Hatは、基本システムライブラリのglibcに深刻なバグがあることを発見しました。glibcはインターネットで広く採用されているライブラリであり、脆弱性のあるバージョンを搭載したサーバーが悪意あるリゾルバーにDNS要求を行った場合、そのDNSサーバーによって要求元のシステム上でコードが実行されるおそれがあります。

セキュリティに脆弱性が見つかったら

Herokuはこのglibcの問題を重く受け止めました。Dynoコンテナのセキュリティを確保するために万全を期し、ユーザーを守るためにあらゆる手段を講じました。

セキュリティインシデントが発生した場合、Herokuではまず、セキュリティチームがすみやかに状況を評価します。セキュリティチームはエンジニアリングチームと協力して、発見された脆弱性がHerokuに与えるリスクの大きさを判断します。今回のケースでは、遠隔操作でコードを実行される可能性があることから、glibcを使用しDNSクエリを行う全システムに、優先度「高」のパッチが必要と判断しました。つまり、ほぼすべてのシステムにパッチの適用が必要でした。

Herokuでは、Common RuntimeプラットフォームとPrivate Spacesプラットフォームのランタイム環境すべてにパッチを適用しました。さらに、ユーザーがDyno内で実行するすべてのコードの安全性を確保するため、Cedarスタックイメージにもパッチを適用しました。最後に、ユーザーのデータの安全性と可用性を維持したまま、データプラットフォーム（PostgresとRedis）にパッチを適用するという、非常に困難な作業も実施しました。

セキュリティ対応事例 – glibcの場合(2)

ダウンタイムを最小限に抑える

Herokuでは、アップグレードや新機能、セキュリティパッチなどをロールアウトする際の基本手順が定められています。こうした手順は、変更が適用されるプラットフォームによって異なります。

Common RuntimeとPrivate Spacesについては、この手順がインフラストラクチャに組み込まれています。新バージョンのソフトウェアをプッシュする際、HerokuではDynoの実行基盤となる新しいベースイメージを作成し、ユーザーのDynoをいったんオフにして、新しいイメージを使用した最新のインスタンスに更新しています。

Herokuのベースイメージは、Herokuのいずれかのコンポーネントに変更を加えるたびに、継続的インテグレーション (CI) パイプラインによって自動更新され、常に最新のUbuntuベースイメージを含んでいます。この新しいベースイメージは、自動テストの際や、ステージング環境の新しいランタイムで自動的に使用されます。Herokuではその結果にもとづいて新しいリリース版を作成し、アップグレードを実行します。具体的には、まず社内の既存のステージング環境に導入し、次にごく一部の本番環境に導入、その後、本番環境全体に展開します。各段階に導入するたび、テストを実施します。

今回のケースでは、パッチ適用済みバージョンのglibcに最新のベースイメージが含まれていることを確認し、通常の段階的アップデートとテストプロセスを手動で実行しました。

では、Dynoについてはどうでしょうか。Dynoはセキュリティを強化したLinuxコンテナで、実行基盤となるベースイメージとは分離されています。Dynoの構成要素は少なく、ユーザーのコード、各言語に固有のビルドパックのほか、Herokuが「スタックイメージ」と呼ぶ要素で構成されています。スタックイメージには、glibcのような基本のシステムリソースを提供する役割があり、常に最新のセキュリティパッチの適用が欠かせません。今回は、glibcのパッチ適用済みバージョンを用意し、すぐにベースイメージを更新すると同時に、スタックイメージを更新しました。これで、Dynoが次に更新されるタイミングで新しいスタックイメージが使用されます。

Dynoの更新サイクルはデフォルトでは24時間ですが、それを短縮する必要があるとHerokuが判断した場合には、更新を早めることができます。今回の場合は、更新するとあらゆる要素が短時間のうちに連続して再起動されるので、ユーザーに混乱が生じないよう、通常の24時間のサイクルまで待つことにしました。発見された脆弱性には、実行中のアプリケーションに影響を及ぼす可能性があるほど高いリスクはないと判断したためです。

セキュリティ対応事例 – glibcの場合(3)

データへの対応

PostgresやRedisなど、データストアの更新はさらに複雑です。ユーザーのデータは決して失われてはならない情報で、Herokuのランタイムのように自由に構築できるものではありません。データの可用性とセキュリティを両立させなくてはならず、サーバーにパッチを適用しながらも、データフローを維持する必要があります。

これを実現するために、Heroku Postgresはユーザーのメインデータベースに送信されるすべてのデータを自動的にコピーする「フォロワー」データベースを採用しています。すみやかに更新が必要な場合、まず最新の状態のフォロワーデータベースを新たに作成し、そのフォロワーをメインのデータベースに変更します。その際、短時間のダウンタイムが発生するため、サービスの中断に備えてユーザーにメンテナンスウィンドウを設定してもらいます。今回のケースでは、脆弱性を評価した結果、ほとんどのユーザーが事前に決めたメンテナンスウィンドウで更新作業を実施しました。

Heroku Redisも同様に、メンテナンスウィンドウを活用しました。こちらもほとんどのユーザーが、事前に決めたメンテナンスウィンドウで更新作業を実施しています。

Heroku自体への対応

Herokuのサービスの多くは、独自のプラットフォーム上で提供されています。Herokuはあらゆるツールを駆使してサービスのセキュリティと安定性を維持しています。今回のケースでは、保守作業の予定を組み、前述のフォロワーを使用した切り替えのプロセスを経て、Heroku内部のデータベースにパッチを適用しました。この保守作業に伴い、各データベース上でHerokuのAPI、デプロイ、オーケストレーションシステムはほんの数分ほど影響を受けましたが、ルーターやランタイムへの影響はなく、エンドユーザーは保守作業中でも必要なアプリケーションにアクセスすることができました。

セキュリティ対応事例 – glibcの場合(4)

すみやかにバグに対応し、ビジネスを継続

セキュリティホールが見つかった場合、パッチの適用は避けられません。glibcに問題が見つかった前年にはGHOSTに、さらにその前年にはHeartbleedに問題が見つかっていました。Herokuは、パッチの適用によってお客様の業務が中断されることがあってはならないと考えています。セキュリティ問題に対処する場合、あるいはプラットフォームの保守を行う際には、できるだけお客様のビジネスやアプリケーションに影響が出ないよう力を尽くしています。

> 今や単なるホスティングサービスやブラックボックスなPaaSを提供するだけでは不十分です。開発者は、パブリッククラウド内でプライベートネットワークを展開し、データをホストするリージョンを選択できるサービスを求めています。
>
> パブリッククラウドはその利便性により支持されていますが、データの保管場所とガバナンスも、ユーザーは同じくらい重要視しています。
>
> Herokuは元来のシンプルさと利便性を維持しつつ、全製品がセキュリティとコンプライアンスに求められる要件を満たすよう取り組んでいます。

RedMonk社創業者
JAMES GOVERNOR氏

salesforce app cloud

事業継続性の確保

可用性が高く、障害に強いHerokuプラットフォーム

Herokuでは重要なデータやシステムはすべてバックアップされ、冗長化も十分になされています。ユーザーのデータはもちろん、機密性の高いデータはすべて暗号化されてバックアップされます。Herokuプラットフォームでは、データのバックアップにテープやディスクといったリムーバブルメディアは使用しません。バックアップはすべて、本番用アプリケーションをホストしている、クラウドインフラストラクチャ上に作成されます。データベースを復旧する際は、標準テンプレートからシステムインスタンスをリストアし、ユーザーのアプリケーションとデータをデプロイして、最新の既知の状態から数秒以内の状態に戻します。

バックアッププロセスは、日頃から継続的にテストされています。プラットフォームを運用する際、ユーザーのアプリケーションとデータベースは繰り返しデプロイされ、プロビジョニング解除され、リストアされます。これがバックアッププロセスの検証作業になっているのです。

標準的なバックアップに加え、Herokuのインフラストラクチャは拡張性とフォールトトレランスを実現するよう設計されています。障害が発生したインスタンスは自動的に置き換えられるため、バックアップからのリストアが必要になる可能性が低下します。

Herokuのコアアーキテクチャ構造は、分散バックアップを使用した障害復旧をサポートしています。コールドサイトをセカンダリとして使用する従来の構成と比べて、この方法には多くのメリットがあります。HerokuのDynoとデータベースはすべて、破棄や複製が容易にできるため、アプリケーションをすばやくスケールアップまたはスケールダウンするだけでなく、新たなインスタンスと完全に置き換えることも可能です。置き換え先を同じデータセンターにすることもできますが、システム停止の影響を避けて、異なるデータセンターを選択することもできます。

いずれかのデータセンターで障害が発生した場合は、データセンタープロバイダーであるAWSがデータセンターの復旧作業を実施します。

Herokuの障害復旧プランは、コンピューティングリソースの作成や削除に伴って継続的に更新され、テストされています。運用チームは、日々キャパシティと可用性の指標をチェックして、どのようなシステム停止に対しても優れた耐障害性を備えていることを確認しています。

salesforce app cloud

テナントのアプリケーション

Herokuプラットフォームにデプロイされたアプリケーションは、デプロイプロセスの一環としてアクセス制御されたセキュアな冗長ストレージ上に自動でバックアップされます。アプリケーションが停止した場合、Herokuではこうしたバックアップを使用して、ユーザーのアプリケーションをHerokuプラットフォームの任意の場所にデプロイし、自動的にオンラインに戻します。この可用性に優れたアーキテクチャを活用するには、適切なアプリケーションやデータベースを設計し、デプロイする責任をお客様が負うことが求められます。Herokuプラットフォームでは、アプリケーションの設計、構築、運用の12の方法論を提唱しており、特に重要なものを以下に示します。

- 依存関係を明示的に宣言し、分離する
- 設定を環境変数に格納する
- アプリケーションを1つもしくは複数のステートレスなプロセスとして実行する
- 高速な起動とグレースフルシャットダウンによって破棄を容易にし、安定性を最大限に高める

Postgresデータベース

Heroku Postgresは、継続的な保護アーキテクチャを活用してデータの安全性を維持しています。データへの変更はすべて先行書き込みログに記録され、複数のデータセンターに置かれた耐久性の高いストレージに分散して保管されます。万一、回復不可能なハードウェア障害が発生した場合には、こうしたログを自動的に「再生」することで、最新の既知の状態から数秒以内の状態にまでデータベースを復旧できます。Herokuは、バックアップ要件とデータ保持要件に合わせて、お客様自身でデータベースをバックアップする機能も備えています。

> 技術情報の詳細については、以下をご参照ください。
> **devcenter.heroku.com/articles/heroku-postgres-data-safety-and-continuous-protection（英語）**

Heroku PostgresのPremium契約およびEnterprise契約のプランはすべて、高可用性（HA）に対応しています。HAは、データベースの可用性を高めるために設計されたデータベースクラスタと管理システムを活用して、ハードウェアやソフトウェアの障害が発生した場合に、ダウンタイムを最小限に抑える機能です。HAが有効になっているプライマリデータベースで障害が起きると、スタンバイと呼ばれる別のレプリカデータベースに自動で置き換えられます。その結果、不具合が生じたデータベースインスタンスは破棄され、スタンバイがプライマリとして再構成されます。

構成とメタ情報

ユーザーの構成とメタ情報は、データベース情報が格納されている、冗長化された堅牢なインフラストラクチャに絶えずバックアップされます。頻繁にバックアップすることで、システムは実行中のアプリケーションに関して、初回のデプロイ以降に加えられた構成の変更点を収集できます。

耐障害性と可用性

Herokuプラットフォームは安定性と拡張性を実現するよう設計されています。そのため、サービスの停止を招くような問題を軽減しつつ、復旧性を維持する工夫がされています。Herokuプラットフォームでは、冗長化によって単一障害点を排除し、障害が発生したコンポーネントを自動的に置き換えます。

Herokuプラットフォームは複数のデータセンターに展開されているため、1か所で障害が発生しても、最新のシステムイメージとバックアップ内に格納されたデータを使用してプラットフォームを復旧できます。サービスに影響を及ぼすインシデントが発生した場合には、Herokuチームが原因とお客様への影響を調べ、プラットフォームの改善策と今後に向けたインシデントの防止プロセスを策定します。

> Herokuのサービスが中断された場合は、重大度の詳細、影響、
> 問題の継続時間をステータスページに掲載しています。
>
> **status.heroku.com（英語）**

事業継続性の確保と緊急時への備え

HerokuはSalesforce製品として、Salesforceがグローバルに展開する事業継続性管理プログラムに準拠しています。このプログラムには、サイトごとの緊急対応計画（ERP）やリージョンレベルとグローバルレベルの危機管理計画（CMP）と連動して、緊急時に組織にとって重要な業務を機能させる事業継続計画（BCP）が含まれています。

また、Salesforceの緊急時準備計画（EPP）には、施設所有者が定めた緊急対応の想定を上回る事態が発生した場合に備えて、緊急時の備えや対応に関する情報、指示、ガイドラインなどが示されており、社員とビジターの健康と安全を守ります。

インシデントへの対応

Herokuクラウドアプリケーションプラットフォームは、自動化された包括的なシステムによって24時間、365日体制で監視されています。Herokuのインフラストラクチャやコアシステム、ツールなどに異常や運用に影響を及ぼす問題が発生した場合は、専任のHeroku運用チームに通知され、問題の診断と解決への取り組みがすみやかに行われます。

サービスに影響を及ぼすような問題が発生した場合は、Herokuプラットフォームのステータスサイト（status.heroku.com）で公開し、問題の影響や対応状況をいち早く伝えます。

万一、データ侵害が発生した場合には、HerokuセキュリティチームがSalesforceのコンピューターセキュリティインシデント対応チームと対応策を協議します。影響を受けるお客様には、Herokuのセキュリティチームができるだけ早い段階で連絡します。インシデントが発生した場合、Herokuセキュリティチームではインシデントコマンダー（IC）が任命され、対応の調整、情報伝達、事後分析の指揮に当たります。

Elements Marketplace

Herokuが管理するHeroku Elements Marketplaceでは、Herokuと連携して使用できるフルマネージドサービスのアドオンや、サードパーティ製のコンポーネントやライブラリ、パターンアプリケーションをワンクリックでプロビジョニング、構成、デプロイできるボタンなどを、Herokuのベストプラクティスを活用して簡単にHerokuプラットフォームに組み込めます。アドオンはシングルサインオンでHerokuとの共通IDを利用するように設計されており、ログも統合されます。ただし、セキュリティやコンプライアンスの要件を確保する正式な検証プロセスは用意されていません。

アプリケーション権限

アプリケーション権限を使用すると、Herokuの組織アカウントに対し、アクセス制御や、アドオンをデプロイする権限などを細かく設定できます。各権限は個別に割り当て可能で、1つのアプリケーションに関する任意の権限を組み合わせて割り当てることができます。これにより、管理者はアドオンの使用を適宜制限し、ソフトウェアの開発プロセスを統制できます。

アドオンによるセキュアなアプリケーション構築

アドオンを活用すると、セキュリティのベストプラクティスに従ったアプリケーションを簡単に設計できます。たとえば、Elements Marketplaceでは、アプリケーションの監視、ロギング、テスト機能を提供するサードパーティ製コンポーネントが複数提供されています。また、静的IPやDNS管理といったネットワークサービスを提供するものや、アラートと通知をサポートするもの、認証やシングルサインオンといったユーザー管理をサポートするものも用意されています。さらに、Webサイトのセキュリティスキャン、SSL暗号化、鍵管理といったセキュリティサービスを行うアドオンも入手できます。

物理的セキュリティ

データセンターへの立ち入り

データセンターへの立ち入りは、ビデオ監視システムや最新式の侵入検知システムをはじめとする電子技術を駆使し、敷地周辺や建物の出入り口に警備員を置くなどして厳しく監視されています。適切な権限を持つ担当者がデータセンターのフロアに入るには、最低3回の2要素認証にパスする必要があります。ビジターや契約業者が立ち入る場合は、身分証を提示して入構許可を得たうえで、権限のある担当者と常に行動を共にする必要があります。

Herokuのデータセンタープロバイダーは、業務上、データセンターへの立ち入り権限が本当に必要な社員にしか、立ち入り許可や立ち入るのに必要な情報を与えていません。データセンターに入る必要性がなくなったときには、立ち入り許可がただちに取り消されます。データセンターへの立ち入りや電子的なアクセスはすべて記録され、定期的に監査されています。

環境の管理

火災の検知と消火

火災のリスクを減らすため、自動火災検知器や消化設備を設置しています。データセンター環境、機械関連や電気関連のインフラストラクチャの設置スペース、冷却室、発電設備室のすべてに、火災検知システムとして煙感知センサーを取り付けています。さらに、こうしたエリアには、充水型、二重連結予作動式、ガス式のいずれかのスプリンクラーシステムが備えられています。

電源

データセンターの電力システムは完全に冗長化され、運用に影響することなく24時間体制で保守できるよう設計されています。また、バックアップ電源として無停電電源装置（UPS）を持っているため、電源障害が発生しても施設内で最も重要で不可欠な部分への給電は確保されます。各データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。

空調と温度の管理

常にサーバーをはじめとするハードウェアに適した運用温度を保ち、機器のオーバーヒートを防止してサービスの停止リスクを軽減するには、空調の管理が欠かせません。各データセンターは空調設備を使って施設内の環境を最適なレベルに維持しています。また、各種の監視システムを導入し、温度と湿度が最適なレベルに保たれるよう、データセンターの職員が管理しています。

管理体制

データセンターの職員は、電気や機械、生命維持関連のシステムや機器を監視し、問題が発生した場合は即座に検知します。また、常に機器を運用できるよう、予防保守を実施しています。

ストレージデバイスの廃棄

ストレージデバイスが耐用年数の上限に達した場合は、権限のない第三者にユーザーのデータが渡ることのないように策定された廃棄プロセスにのっとって処理されます。Herokuのデータセンタープロバイダーでは、こうした廃棄プロセスの一環として、DoD 5220.22-M（National Industrial Security Program Operating Manual – 国家産業セキュリティプログラム運営マニュアル）またはNIST 800-88（Guidelines for Media Sanitization – 媒体のサニタイズに関するガイドライン）に規定された方法で、完全にデータを消去しています。廃棄処分する磁気ストレージデバイスはすべて、業界の慣例に従って消磁され、物理的に破壊されます。

> 柔軟に運用できるHerokuのおかげで、法規制に準拠した安全性の高いサービスを提供できるようになりました。更新プログラムの適用もすばやく簡単に行えるようになり、本当に助かっています。

LendUp社CTO
JAKE ROSENBERG氏

コンプライアンスと監査

Herokuの物理インフラストラクチャはAmazonのセキュアなデータセンター内でホストされ、アマゾンウェブサービス（AWS）テクノロジーを活用して管理されています。Amazonは継続的にリスクを管理し、繰り返し評価して、業界標準のコンプライアンスを満たしています。Amazonはデータセンターの運営に関して、以下の認証を受けています。

- ISO 27001:2013 – ISO 27002のベストプラクティスに関するガイダンスに従って、セキュリティ管理のベストプラクティスおよび包括的なセキュリティ統制について規定したセキュリティ管理標準
- ISO 27017:2015 – 国際標準化機構（ISO）からリリースされた最新の実施基準で、クラウドサービスに特化した情報セキュリティ統制の実施に関するガイダンスを提供
- ISO 9001:2008 – 製品およびサービスの品質管理に対する世界標準で、国際標準化機構（ISO）の品質管理および品質保証に関する技術委員会によって定義された8つの原則にもとづき、品質管理システムについて規定
- SOC 1、SOC 2/SSAE 16/ISAE 3402（以前のSAS 70 Type II）、SOC 3 – 独立した第三者機関による審査報告書で、主要なコンプライアンスの内部統制と目標をAWSが達成したことを証明
- PCIレベル1 – ベストプラクティスとさまざまなセキュリティ統制について規定したクレジットカード業界のための標準で、セキュアなネットワークの構築と保守、カード所有者のデータ保護、脆弱性管理プログラムの保守のほか、強力なセキュリティ対策の実施、ネットワークの定期的なテストと監視、情報セキュリティポリシーの保守を求める
- FISMA Moderate – 連邦情報セキュリティマネジメント法（FISMA）の準拠を外部の評価機関が証明

> 最新の監査レポートと証明書については、SalesforceまたはHerokuの営業担当者にお問い合わせいただくか、以下のリンク先をご参照ください。
> **aws.amazon.com/compliance**

Herokuを実行するインフラストラクチャであるデータセンターの認証に加え、Salesforceは現在、PCI DSSレベル3の認証および医療保険の携行性と責任に関する法律（HIPAA）への準拠を目指しています。この認証はHerokuのコアサービスにも拡張され、また、適切なセキュリティ統制策を施したアプリケーションの設計方法に関する規範も含まれています。

> HerokuではPCI DSSレベル3の認証に先駆け、Herokuプラットフォーム上でサードパーティの決裁処理サービスを活用してPCIに準拠したアプリケーションを構築する方法についてガイドラインを示しています。
> **devcenter.heroku.com/articles/pci-compatible-apps（英語）**

おわりに

Heroku Enterpriseはクラウドでの開発を可能にするプラットフォームサービスです。そのため、初期段階からスタックの各層でセキュリティ対策を実施できるよう設計されています。物理セキュリティやネットワークセキュリティから、Herokuのマイクロサービスアーキテクチャおよびコンテナベースのデプロイモデルまで、プラットフォームの管理やセキュリティ対策はSalesforceが担うため、お客様はビジネスアプリケーションの構築に専念できます。

> HerokuおよびSalesforce App Cloudについては、以下のサイトをご参照ください。
>
> **salesforce.com/jp/platform/products**