

Keycafeセキュリティ・アーキテクチャの概要について

バージョン 4.0 | 最終更新日: 2026年9月

はじめに

Keycafeは、多くのビジネスにおける使用例においてカバーできるセキュリティレベルを維持しながら、ビジネスにおいて鍵をリモートで管理する便利な方法を提供します。製品設計をはじめ、システムアーキテクチャ、頑丈なSmartBoxのデザインまで、弊社のソリューションは、セキュリティ、利便性、ユーザービリティのバランスを考慮し、一から設計されております。この概要では、Keycafeのスマート・キーマネジメント（鍵管理）プラットフォームに組み込まれた、必要不可欠なセキュリティ機能についてご紹介します。

業界最高水準のサーバー、アプリケーション、データベース・アーキテクチャを提供

最新のサービスとセキュリティ

Keycafeはトップレベルのサービスプロバイダーと連携して、最先端のセキュリティを提供しています。トランスポート・レイヤー・セキュリティ、DDoS攻撃防御、ファイアウォール管理はKeycafeのデータサーバー構築に欠かせない要素です。Keycafeはパスワードのハッシュ化、アクセスログ、ソースコードのレビュー、侵入テストなど、強固なセキュリティ基準に沿って運営されています。



トランスポート・レイヤー・セキュリティ

TLS、各種認証、データインTEGRITY照合によって、不正アクセス・データ改ざんを防御しています。利用者のパソコンとKeycafeとのコミュニケーションは保護されており、アカウント管理に関わる全ての情報は安全に受信されます。



DDoS攻撃防御

Keycafeへのアクセスは、トップクラスのCDNパートナーによりサービス拒否攻撃(DDOS)から保護されています。67Tbps以上のネットワーク容量を持つCloudflareは、一日あたり平均70Bの脅威をブロックし、最大かつ最も仕組まれた攻撃から、お客様のアクセスを保護します。



ファイアウォール管理

複数の最新型ファイアウォールにより、お客様のデータは保護されています。ファイアウォールは、機密データのより引きを含むネットワーク・トラフィックを保護するために必要不可欠です。これらのシステムは、PCI DSS、HIPPA、GDPRなどの法令を遵守するために必要です。



PCIに準じた決済プロセス

お客様の決済情報は、業界内で最も厳しいとされるPCI Service Level 1の認定を受けたPCIに準じた決済代行サービスによって暗号化されています。



脆弱性のテスト

Keycafeでは、自動化された侵入テストを定期的に行い、悪用される前にシステムにおける脆弱性を発見しています。セキュリティエキスパートの方々が設計したこのテストは、実際のハッカーの行動をシミュレーションし、サーバーにおける設定ミスや、SQLインジェクション、クロスサイトスクリプティング、公開ファイル/ディレクトリ、脆弱な暗号化プロトコルやサイファーなどの問題点を指摘します。また、一般的なソフトウェアやプロトコルの既に把握されている脆弱性(Heartbleedなど)をテストします。

Keycafeには、業界最高水準のモニタリングと、自動脆弱性診断機能を提供するソフトウェア提供会社のソフトウェアが組み込まれています。以下に、Keycafeのソフトウェア提供会社を掲載します。



クラウドフレア

DDoS防御、レート制限、CDNパフォーマンス向上のためのプロキシ、DNS管理において、世界的最高の水準保持しています。Cloudflareは2千5百万ものインターネットユーザーのプロパティを保護し、信頼を受けています。



ヘロク

ウェブホスティング、システム管理、Linuxセキュリティ/データベースセキュリティアップデート、ファイアウォール、ソフトウェア侵入の検知のための高度なセキュリティを提供しています。HerokuはISO 27001, 27017, 27108に準拠し、SOC 1,2,3に関する報告がされています。[続きを読む](#)



Hologram

世界中で展開されるデバイスの安定稼働からスムーズな拡張、セキュリティ保護までをしっかりと支える、高度で拡張性に優れたセルラーIoTソリューションを提供します。



Intruder.io

Intruder はデジタルインフラストラクチャにおけるサイバーセキュリティ上の脆弱性を発見するクラウド型脆弱性スキャナです。

Keycafeは Intruder.io による脆弱性スキャンを毎日実施しており、10,000件以上の攻撃手法（アタックベクター）に対する耐性テストにおいて「A+」評価を獲得しています。



ストライプ

オンライン上での請求プラットフォームにおけるリーディング・カンパニーです。スタートアップ会社から大企業まで、数百万のあらゆる規模の企業が、PCIに準拠したStripeのソフトウェアとAPIを利用して、支払いの受付、送信、オンライン上でのビジネス管理を行います。

サービスレベル契約 (SLA)



99.9%の稼働率（アップタイム）を保証します。[詳細を読む](#)

コンプライアンスおよび継続的なモニタリング

Keycafeは Drata を活用し、SOC 2、GDPR、および関連するプライバシー/セキュリティフレームワークへの準拠を自動化・監視しています。Keycafeは独立した第三者機関による「SOC 2 Type II」および「SOC 3」の認証を受けています。これらの認証は、当社のセキュリティ管理およびプロセスが、お客様のデータを保護するための業界最高水準を満たしていることを証明するものです。Drataは管理状態をリアルタイムで監視し、当社のシステムおよびポリシーが常に監査可能な状態に保たれるよう維持します。各種認証やレポートについては、[Keycafe Trust Center](#) をご覧ください。



プライバシーポリシーとデータ処理

GDPR準拠

Keycafeの[プライバシーポリシー](#)は、どのような情報が収集され、どのように使用、共有、保護、保管されるかの概要を定めています。Keycafeはカナダのバンクーバーに拠点を置いており、お客様のデータはGDPRコンプライアンスプログラムに準拠した信頼できるサードパーティのクラウドプロバイダーによって処理および保管されます。クラウドプロバイダーは、お客様情報の管理方法を定めたデータ処理契約に基づいて運用されています。

Keycafeの「[データ処理補足契約\(DPA\)](#)」は、最新のプライバシー基準に準ずるためにアップデートされています。各種法令に沿って、顧客データがどのように保護されているかが明記されています。

ユーザー認証とアクセス権

お客様のご要望に合わせたアクセス認証システム

Keycafeのユーザー認証では、賃貸物件、車両、社内施設にアクセスするユーザーを管理するためのオプションを多数用意しております。ID番号とSNSメッセージで送信されるアクセスコードの入力が必要な二段階認証が、初期設定において有効になっています。

お客様の契約プランに応じて、管理コントロールや、スケジュール設定、バッジスキャンなどの、カスタマイズされたさまざまなアクセス権をユーザー認証に追加することが可能です。お客様のSmartboxのユーザー認証オプションをフル活用し、ユーザーの方々ごとに合わせたアクセス権を設定することは、鍵への不正アクセスに対する重要な抑止力となります。

以下は、アクセス可能なオブジェクトの種類と、アクセス権が付与/管理可能なアクセス権オプションの表です。

オブジェクト/アクセス権の種類	説明	鍵にアクセスできるユーザー	ユーザー認証
キーコード	Smartboxにおいて入力すると鍵の有無が分かる、任意の鍵に対して作成できるシンプルなコードです。鍵が引き出されるまでキーコードは有効です。	キーコードを渡した人	SmartBoxでキーコードを入力します。
スケジュール化された予約システム	限られた期間内において鍵へのアクセスが可能で、登録ユーザーでなくても鍵が使用可能です。	予約の詳細を伝えた人	SmartBoxで予約コードを入力、もしくは独自のURLを活用することで、使いやすい認証システムを提供します。
シングルキー・アクセス権	ユーザー、またはユーザーグループに対して、特定の鍵にアクセスするための、データベース上のアクセス権限です。	鍵を交換、または管理する権限を与えられたユーザー/ユーザーグループに属する全てのユーザー	KeycafeのiOS/Androidアプリを使用、もしくはSmartboxでIDコード、さらに2段階認証コード(必要な場合は設定)を入力します
全ての鍵の使用許可	ユーザーまたはユーザーグループが、彼らのアカウントが所有する全ての鍵にアクセスするための、データベース上のアクセス権限です。	全ての鍵グループを交換、または管理する権限を与えられたユーザー/ユーザーグループに属する全てのユーザー	KeycafeのiOS/Androidアプリを使用、もしくはSmartboxでIDコード、さらに2段階認証コード(必要な場合は設定)を入力します
カスタマイズされた鍵のグループ	ユーザーまたはユーザーグループが、指定された鍵のグループにアクセスするための、データベース上のアクセス権限です。	鍵の交換の権限を持つユーザー、カスタム鍵グループの管理者権限を持つユーザー/カスタム鍵グループの交換権限または管理者権限を持つユーザー/ユーザーグループ	KeycafeのiOS/Androidアプリを使用、もしくはSmartboxでIDコード、さらに2段階認証コード(必要な場合は設定)を入力します
鍵の保管ケース	鍵へのアクセス権に関係なく、ユーザーがSmartBoxの鍵の保管ケースをリモートで開けることができる機能です。	鍵の交換場所における管理者権限を持つユーザー	KeycafeのWeb/iOS/Androidアプリを使用します。
SmartBoxのメインロック	鍵のアクセス権に関係なく、Smartbox全体をリモートで解錠することができる機能です。	鍵の交換場所における管理者権限を持つユーザー	KeycafeのWeb/iOS/Androidアプリを使用します。

IoTサーバーとSmartBoxとの通信

頑丈でダイナミック、そして有益

KeycafeのIoTセキュリティは、Particle(前述)のデバイスクラウドと連携することで、ISO 27001、27012、27018の物理セキュリティとリスクマネジメントを備えた、トップクラスのホスティングに支えられ、サービス層とデータの両方で攻撃され得る領域を最小化することができます。



進化したIoTセキュリティ

SmartBoxと弊社のサーバー間は全て暗号化されており、安心してご利用いただけます。受信ポートをオープンにしていないので、ポートスキャナーやサイドアタックを阻止することができます。各デバイスには固有の暗号が備えられており、包括的なセキュリティ監視により、潜在的な脅威からサーバーを保護します。



暗号化された無線接続

SmartBoxとのブルートゥース通信は転送中も完全に暗号化されています。WiFi接続に関しては、業界標準のWPA2を使用しており、セキュリティが確保されています。携帯電話との接続に関しては、業界標準の暗号を使用し、全てのデータの転送を安全に行います。



端末の動作アラート

24時間365日稼働のSmartBoxクラウド接続により、鍵の交換は自動的にメール、モバイル通知、Webhookを通して、リアルタイムに詳細な通知を送信します。ユーザー認証はサーバーと通信にてライブで行われるため、Keycafeは鍵へのアクセスをリアルタイムでコントロールできます。



OTAアップデート

各SmartBoxは無線を介してアップデートを受けるため、ファームウェアとセキュリティ機能は常に最新の状態で保たれ、新たな脅威に対しても、先手を打つことができます。

SmartBoxの構造について

SmartBoxの強度

鋼板で固定されたSmartBoxは、耐久性に優れた16ゲージ(約1.5mm厚)の粉体塗装スチールフレームを採用しています。内部では、個々の鍵キャビネットが独立したダイカスト金属ドアで囲まれています。電子マスターロックは外部からアクセスできず、視界からも完全に隠されています。頑丈な金属構造、個別の鍵キャビネットごとのロック、および外部に露出したマスターロックがない構造により、計画性のない悪意ある改ざんや誤用を強力に防ぐ設計となっています。また、屋外に設置する場合の更なるセキュリティ向上として、南京錠等を取り付け可能なループが付いた「屋外用スチール製カバー(屋外カバー)」もご用意しています。

使用用途とセキュリティ

KeycafeのSmartBoxは「金庫」ではなく、執拗な盗難攻撃に耐える設計や評価(耐火・耐工具等級等)を受けているものではありません。また、リレーアタック/リプレイアタック、鍵の複製、あるいは信号増幅攻撃を防ぐ機能を備えているわけではありません。実用上、正式な定格評価を受けた金庫であっても、意図的な盗難に対して耐えられるのは一定時間に過ぎません。本製品は、追跡可能性(ログ管理)と責任の明確化を強化することにより、使いやすさ、利便性、そしてセキュリティを提供するよう設計されています。SmartBoxは、盗難のリスクが低いと思われる、十分な照明と監視設備(防犯カメラ等)が整った環境でのみご使用ください。また、SmartBoxの使用や設置場所が保険請求にどのような影響を与えるかについては、ご契約の保険会社にご確認いただく必要があります。自動化された、無人での鍵の受け渡しという利便性が、お客様のユースケースやニーズに適しているかどうかは、お客様ご自身でご判断ください。その他のセキュリティに関するアドバイスについては、Keycafe利用規約をご確認ください。

SmartBoxの特徴：

- 16ゲージスチール背面パネルを壁に固定
- 20ゲージスチールで補強された高精度成型ポリカーボネートフレーム
- 鍵キャビネット蓋はA383合金 ダイキャストメタル製
- 内蔵監視カメラ
- マスターアクセスにより鍵収納スペースにアクセス可能
- 耐候性粉体塗装
- 屋外設置用スチール製カバーのオプション

前述の最先端のIoTセキュリティ、カスタマイズ可能な認証ワークフロー、およびクラス最高峰のソフトウェア連携によって、SmartBoxはさらに保護されています。

その他の情報について

弊社のサポート/セールスチームは、弊社の製品に関連する幅広い技術的トピックについて、最善を尽くした状態で対応させて頂いておりますが、その回答が必ずしも的を得ていたり、最新情報に対応していない場合がございます。この文章では、弊社のセキュリティアーキテクチャ/プラクティス、およびキーベンダーの概要について、詳細に説明します。この文章において記載されていないセキュリティに関する質問で、明確な回答が必要な場合は、security@keycafe までご相談ください。弊社のプロダクトリーダーやエンジニアに相談し、お客様にさらに詳しい情報を提供します。

