SmartBox セキュリティ

Keycafeセキュリティ・アーキテクチャの概要について

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、データインテグリティ照合によって、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送信されます。

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ーウォールにより、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**

Intruder.io

Intruderは、一万もの典型的な攻撃ベクトルをスキャンすることで、デジタルインフラにおけるサイバーセキュリティの脆弱性を発見できる、クラウドベースの脆弱性スキャナーです。

パーティクル

IoT業界をリードするこのプロバイダーは、リモートデバイス、ハードウェア、クラウドサービスから構成される安全性の高いネットワークの管理を可能にします。

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。

Keycafeは、Intruder.ioによる一万以上の攻撃ベクトルを対象としたスキャンで、99.98%のセキュリティ対策の有効性スコアを打ち立て、A+を獲得しました。

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、データー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、データー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、データー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、新たなる脅威に対しても、先手を打つことができます。

機密データのオフサイト化

Keycafe Smartboxには、機密データは一切保存されません。一方で、暗号化プロトコルによって保護レイヤーが追加されます。

個人情報保護方針とデータ処理

GDPRに準拠

Keycafeにおけるお客様重視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、保存されるかを概説しています。Keycafeはカナダのバンクーバーに本社を構え、お客様のデータは施設内では処理されません。当社は、トップクラスである、第三者のクラウド・サービス・プロバイダーにお客様の情報の処理と保存を委託しており、アメリカ、カナダ、ヨーロッパ連合、その他の国においてプロバイダーがお客様の情報の処理と保存を行う場合がございます。弊社では、プロバイダーがGDPRコンプライアンス・プログラムを実施していることを確認し、弊社に代行してお客様のデータの処理を制限/規制するデータ処理に関する契約を弊社のサービスプロバイダーと締結しています。

弊社のシステムでは、ユーザーの権限と当事者間の暗黙の関係に応じて、どのデータを他のユーザーに表示するかを決める規制と保護措置が含まれています。加えて、弊社のチームメンバーには、デフォルトによりユーザーの個人情報を開示せず、再認証なしで許可される個人情報の表示回数を制限するといった、ワンランク上の内部統制をデータ保護のために行なっています。当社のプライバシーポリシーに関する全文は、こちらからご覧いただけます。

SmartBoxについて

改ざんへの抑止力

スチール製の板で覆われたSmartboxは、40センチの粉体塗装が施された頑丈なスチールフレームが特徴です。内部には、独立したダイキャスト・メタル製の筐体で構成された個々の鍵保管スペースがございます。電子マスターロックにはアクセスできず、完全に見えないようになっています。SmartBoxは、頑丈な金属製の構造、個々の鍵収納スペースのロック、マスターロックが外面に設置されていないことから、アクセス権のない第三者による改ざんを防ぐことができます。

KeycafeのSmartBoxは、例として駅にあるロッカーや、街中で使用されている自転車ロックと同様のセキュリティレベルを想定しています。工具を使用する侵入者/泥棒に対応できるレベルではございません。貴重品を保護するための公的な盗難防止認証を受けた金庫は、盗難に対抗できる時間(通常10分以内)でその硬度を測定しているので、例え最も安全な金庫であっても、実際には悪意ある人物に対抗できる時間は限られています。弊社の製品は、金庫や保管庫などではなく、使いやすさと利便性を重視した上で、堅牢な構造をしています。SmartBoxは明るくて監視可能、盗難の可能性が低いと思われる環境のみで使用してください。SmartBoxの使用や設置が、保険金請求にどのような影響を及ぼすかについては、保険会社にご相談ください。

SmartBoxの特徴:

- 15本ネジのスチール製プレート装備
- 16ゲージ冷却圧延スチールフレーム
- A383合金ダイキャスト金属製、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

各SmartBoxは、上記のように、最先端のIoTセキュリティ、テーラーメイド認証、トップクラスのソフトウェア統合によってさらに保護が施されております。

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。