EC-CUBE唯一の「公式」決済代行サービス

「EC-CUBEペイメント」のご案内







株式会社イーシーキューブ GMOペイメントゲートウェイグループ

GMOペイメントゲートウェイ会社概要



■店舗数



■決済処理件数/流通金額

13.6億件

3.4%円



■従業員数/グループ会社数



756人



25社(+持分法3社)

※2018年9月末現在

参照:第25期年次報告書

https://corp.gmo-pg.com/newsroom/pdf/181217_gmo_pg_ir_nenjihokoku.pdf

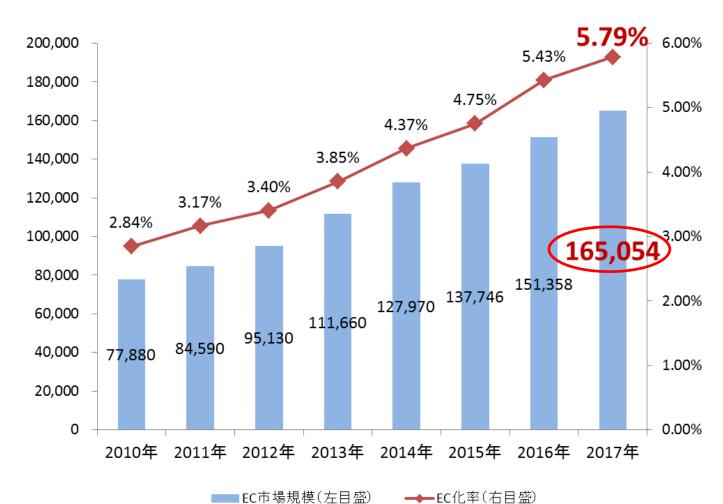
参照:2019年9月期 第1四半期決算説明会

https://corp.gmo-pg.com/newsroom/pdf/190214_gmo_pg_kessan.pdf

昨今のキャッシュレス事情



- 日本国内のEC市場は年々増加。
- →BtoC-EC市場規模は16.5兆円(前年比9.1%増) BtoB-EC市場規模は317兆円(前年比9.0%増)



「平成29年度我が国におけるデータ駆動型社会に係る基盤整備(電子商取引に関する市場調査)」 経済産業省

E C 京・中央)は電子商取引ミック経済研究所(東 代行サービスについ 向けのネット決 ト販売 決済代行市場 場規模は6120億円と 化の推進により 府によるキャッ 大きく成長すると分析 調査は国内のネット決

国内23年度

供する。 の決済処理システ ドやコンビニ決済 クレジッ

済代行業者を対象に売り

決済代行業を後

2019/05/13日経MJ(流通新聞)11ページ

EC-CUBEペイメントとは?





EC-CUBEペイメントは、 EC-CUBE「公式」決済の 信頼の決済代行サービスです



EC-CUBE開発元の株式会社イーシーキューブと、決済代行業界No,1のGMOペイメントゲートウェイグループ(東証一部上場、2019年3月末現在133,199店が利用中)が資本業務提携を行いサービス提供しており、現在1,000店舗以上のクライアント様にお使いいただいております。

















※バージョン、プラン により非対応の決済 手段がございます。

EC-CUBEペイメントの特徴



FILLIBE の 4つの特徴 Payment



①管理画面連携

基本の決済管理業務をEC-CUBE管理画面上で行えます。EC-CUBEと決済システムの両方の管理画面にログインや各種確認・処理をする業務の煩雑さを軽減します。

※一部の処理においては、決済システムの管理画面も利用



③モジュール簡単設定

モジュールはプレインストール済み。

別途ご案内の各種アカウント情報設定だけで すぐにご利用いただけます。設定等の煩雑さ を軽減し誰でも使える決済環境を実現します。



②トークン決済

購入者が入力するクレジットカード番号を、 別の文字列(トークン)に置き換えて通信を 行い、お支払いを完了させる、情報漏えいリ スクをより軽減することができます。



④定期購入機能

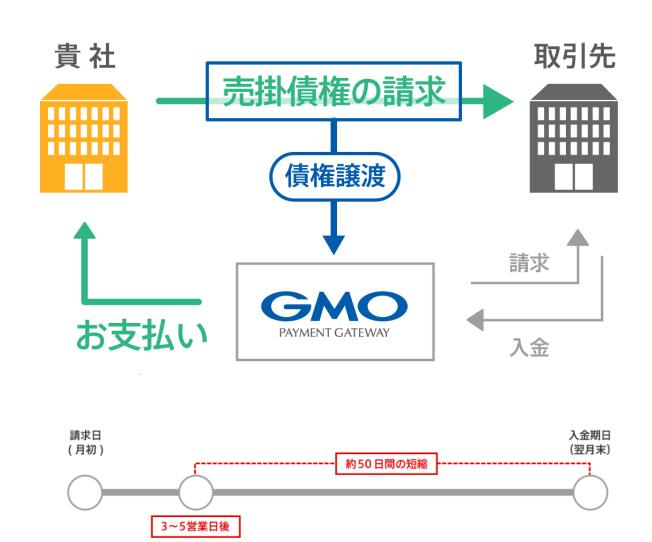
継続購入プラグインをインストールし、 登録したクレジットカードから定期的に 引き落としを行う機能です。お店の安定した ストック型の収益に貢献します。

※バージョン、プランにより非対応の決済手段がございます。

その他サービス 〈GMO BtoB早払い〉 し FC CUBE



保有する売掛債権を買い取ることで、 入金期日よりも早期に資金化することのできるサービスです





くご参考情報> 改正割賦販売法と セキュリティ対策について

ご参考: セキュリティ対策



- ・昨今、EC加盟店等を狙った不正アクセスによりカード情報の漏洩が拡大。
- ・これに伴い、偽造カードやネット上での本人なりすましによる 不正使用被害が増加(2016年で年間約142億円)。
- ・不正使用は国境を越え、犯罪組織に多額の資金が流出しているとの指摘あり。

被害② クレジット取引の不正使用額の推移 クレジット取引での被害イメージ 磁気ストライプでの決済 142.0 2016年:142億円 (億円) (4年間で約2.1倍) 偽造カード不正使用被害 130 不正アクセス 120 110 対面加盟店 120.9 100 90 EC加盟店 114.580 被害① 不正使用者 70 78.6 セキュリティ対策が不十分 被害(3) 60 68.1本人確認なし 50 カード情報の漏えい被害 2011年 2012年 2013年 2014年 2015年 2016年 (注) 不正使用被害額は、国内発行クレジットカードでの不正使用分で、カード会社が把握している分 なりすまし使用被害 を集計(海外発行カード分は含まれない。)。 出所:一般社団法人日本クレジット協会「クレジットカード不正使用被害の集計結果について」

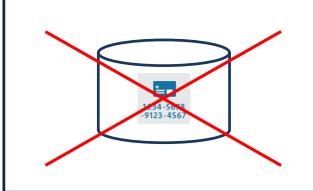
改正割賦販売法(非対面分野)



2020年東京五輪に向け、セキュリティ環境を国際水準へと整備することを目指し、カード情報セキュリティ対策を 義務付ける改正割販法が2018年6月施行されました。

PCI-DSSに準拠しない場合に義務付けられる「カード情報非保持化」は、改正割販法の実務指針として、クレジット取引セキュリティ対策協議会より発表された「実行計画2017」にて定義されています。

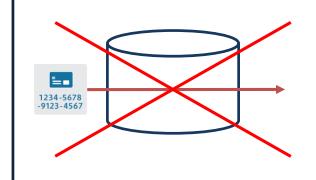
カード情報保持の禁止



【保持の例】

- ・顧客管理などデータベース での保持。
- ・エクセルなど電子ファイル での保持。
- ・メールサーバーでの保持。
- ※音声データ、紙媒体等は 「保持」に該当しません。

カード情報通過の禁止



【通過の例】

・カード情報を含む決済電文の サーバー内通過。

カード情報処理の禁止



【処理の例】

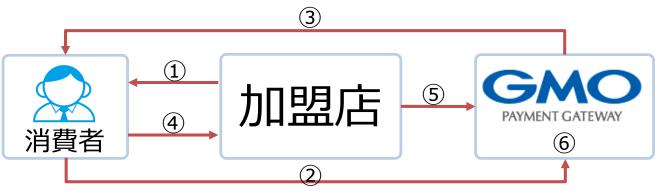
- ・PCIDSS非準拠環境のPCから 決済代行会社の管理画面に 対してカード情報入力。
- ・PCIDSS非準拠環境のPCから 消費者に代わり非保持化EC サイトへカード情報入力。

不正対策ソリューション



カード番号非保持化ソリューション:トークン

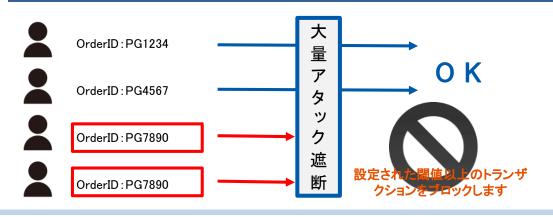
- ・加盟店サーバーにはトークン(暗号化された文字列)が通過しますので、非保持化扱いとなります。
- ・加盟店サイト内にてカード情報の入力が行えるので、サイト遷移などによるカゴ落ちが防止できます。



- ①決済フォーム(カード番号入力画面)
- ②カード番号を弊社提供のJavaScriptが直接取得
- ③無意味文字列(トークン)をブラウザに返却
- ④トークンを加盟店へ送信
- ⑤決済情報連携
- ⑥トークンからカード番号へ復元し、決済処理

大量アタック遮断サービス

- ・加盟店様が設定した検知ロジックに応じて大量のオーソリトランザクションを遮断するサービス
- ・クレジットマスターの被害を予防することができます。(他人のカード番号を割出す手口)



- ・同一オーダーIDに対してn分以内にm回 リトライされたらブロック
- ・同一ショップでn分以内に同一カード番号を 使ってm回リトライされたらブロック などが指定いただけます。