



CREATE company newsletter

THE MARON-E TIMES

〒889-0601 宮崎県門川町須賀崎4-39-3 TEL: 0982-63-7706 Mail: create-info@create-m.co.jp https://create-m.co.jp



2025.06.04(Wed)

クリエート通信



農産物直売所系DX推進 最先端情報



IT導入補助金の申請が始まっています！



申請時に準備しておくこと

● IT導入補助金申請の必須条件

IT導入補助金を申請するにあたって、次の条件を満たしておく必要があります。事前準備が必要なもの、および補助事業完了後に必要なものがありますので、申請を予定している事業所はあらかじめ準備・計画しておくことをお勧めします。

・gBizIDプライムアカウント

法人代表者ご自身または個人事業主ご自身がG Biz IDを取得し、1つのID・パスワードで様々な行政サービスにログインできるサービスです。

・SECURITY ACTIONの宣言

中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度です。「SECURITY ACTION」の「★一つ星」または「★★二つ星」いずれかの宣言を行うこと。また、宣言内容の確認に際し、事務局が一部の交付申請情報を独立行政法人情報処理推進機構（IPA）と共有することに同意することが条件とされています。

・IT戦略ナビwithの実施

中小機構が運営するデジタル化支援ポータルサイト「デジwith」における「IT戦略ナビwith」を交付申請前に行っている場合、加点の対象となります。「IT戦略ナビwith」実施時に、本事業の申請に用いたG Biz IDプライムを入力し、結果が表示された画面を交付申請時に添付することが必要です。（IT戦略ナビwithとは？）→<https://digiwith.smrj.go.jp/it-map/>

・履歴事項全部証明書・納税証明書

法人申請の場合に必要な書類です。個人事業主の場合には、運転免許証か住民票、確定申告書Bが必要書類になります。

・申請時に記載する各種情報

法人番号 / 従業員数 / 業種コード（日本標準産業分類） / 財務状況（売上高、粗利率、営業利益、経常利益、減価償却費、年間平均労働時間、従業員数、資本金など） / 経営状況 etc…



インボイス対応が必須の企業様、特に従業員5名以下の小規模事業者様には補助率が高く、使い勝手の良い補助金となっています。店舗POSレジシステムのインボイス対応をご検討中であれば弊社までご一報ください。

コーポレートサイト改修案件

年度初のコーポレートサイトの改修案件が増えています！

最近のサイト改修のトレンドは…

- ・動きのある動的なデザイン
- ・スマホでの閲覧にも最適なレスポンシブデザイン
- ・セキュリティを強化した安全なサイト構築 です。

クリエートでは、WEBサイト専門の実績豊富なデザイナーを抱え、LP制作等を多数手がけております。インパクトのある動きがありつつ、繰り返し訪問しても飽きることのないUI/UXで、PCでもスマホでも破綻しない熟考されたデザインを強固で安全なシステムで構築可能です！

このようなサイト構築をご希望でしたら是非、弊社までお気軽にお問い合わせください。



ホームページにて、制作実績を公開しております！
(QRコードからアクセス)



食の「安心・安全」への取り組み

Miz Crop

作物の栽培履歴シートを簡単にデータ化し、農薬の基準や肥料の使用状況も自動でチェック・管理！

Miz Cropは作物栽培履歴シートをスキャナーで読み取り、OCRでデータ化、クラウドへデータを収集し農薬の使用基準や肥料の使用状況を自動チェック・管理します。農薬の知識を持たない店舗スタッフでも正確なチェックができるように開発した道の駅、直売所向けのソリューションです。

ハサレポ

24時間 365日自動計測で定期点検や異常時対応を省力化！

ハサレポは冷凍・冷蔵設備の温度や食品加工時の温度を、センサーで常時計測してパソコンやスマホからいつでも確認できる温度管理システムです。温度計測を自動化し、多拠点の温度管理業務を効率化できます。



契約期間中は
無制限でデータ保存



センサー設備に
配線工事やWi-Fi不要



IP67の防水対応で
水がかかっても安心



スマホ通知台数の
制限なし



ホームページの安全のお話



すでに多くの会社様・店舗様がホームページをお持ちのことと思いますが、セキュリティ対策は行われてますでしょうか。近年では、サイトやSNSの乗っ取り被害なども増えており、高額な被害額も出ていると調査で報告されています。

乗っ取り手法も巧妙化してきてますので、今一度対策などのご確認をお勧めいたします。
基本的な対策について列記します。

(1).技術的な対策

- ・ HTTPS (SSL/TLS証明書の使用)
- ・ ウェブサイトとユーザー間の通信を暗号化し、データの盗聴や改ざんを防ぎます。
- ・ URLが「http://」ではなく「https://」で始まることを確認しましょう。

(2).WAFの導入(Web Application Firewall)

- ・ SQLインジェクション、クロスサイトスクリプティング(XSS)などの一般的なウェブアプリケーションの脆弱性を悪用した攻撃からウェブサイトを保護します。
不正な通信を検知・遮断する役割を果たします。

(3).ソフトウェア・システムの定期的なアップデート

- ・ OS、ウェブサーバー、CMS (WordPressなど)、プラグイン、ライブラリなど、ウェブサイトを構成するすべてのソフトウェアを常に最新の状態に保ちます。古いバージョンには既知の脆弱性が含まれている可能性が高いため、セキュリティパッチがリリースされたら速やかに適用しましょう。

(4).ログの取得と監視

- ・ ウェブサーバーのアクセスログやエラーログ、WAFのログなどを取得し、定期的に監視することで、不審なアクセスや攻撃の兆候を早期に発見できます。

(5).バックアップの定期的な取得

- ・ 万が一、攻撃を受けてデータが破損したり消失したりした場合に備え、ウェブサイトのデータ(ファイル、データベース)を定期的にバックアップし、安全な場所に保管しましょう。

ホームページ標準制作費

【基本サイト】※消費税別途

(ドメイン取得/サーバー設置/5ページテンプレート)

●初期設定費：**¥49,800**

●月額保守サポート費用：**¥3,200**

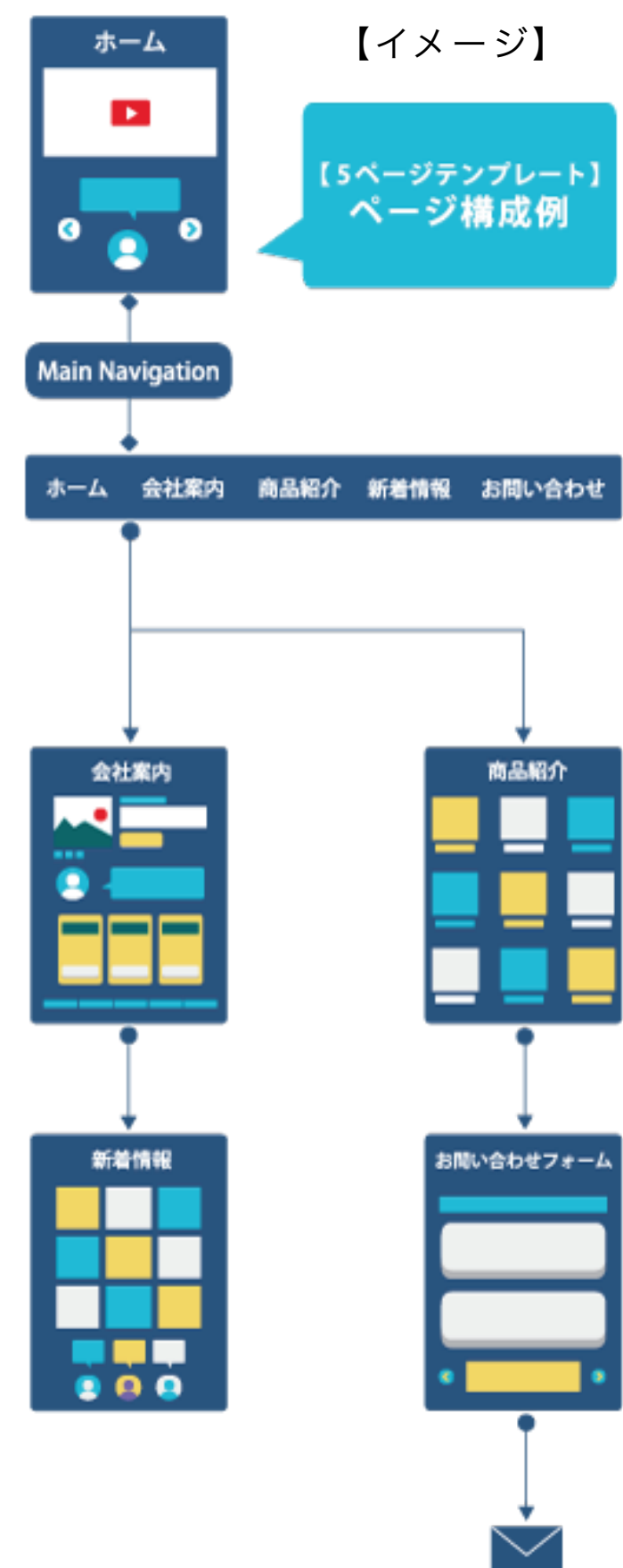
●コンテンツ制作費：**¥340,000**

*基本サイト公開時合計：**¥393,000**

(SSL対応/レスポンシブデザイン/お問い合わせフォーム)

*5ページテンプレートページ構成例

(トップページ/会社紹介/商品紹介/新着情報/お問合せ)



セキュリティ対策には専門的で総合的な知識が必要になります。

手軽にホームページの作成ができる時代ですが、お客様を保護し信頼性の高い情報を届けるためにも、Pマークを取得しているなど基本的なセキュリティ対策が整っているベンダーにご相談ください。