要件定義書

2018/8/30

ECC ティーシャツ株式会社　野島

目次

1 システム導入の目的と目標 2

2 システムの構想／システムの概要 2

3 機能要求 4

4 入力要求と出力要求 9

5 システム導入後のフロー 12

6 品質・性能要求 12

7 インフラ設計要求 13

8 アプリケーションセキュリティ要求 15

9 OS/ ミドルウェアに関するセキュリティ要求 17

10 運用 17

11 パックアップ要件 18

12 保守 18

13 参考資料 19

1 システム導入の目的と目標

お客様がよりわかりやすく買えるよう最適な UI/UX を施し、マイページ上にて
制作のやり取りを実施するほか、決済や再注文が行える仕組みとします。
また、社内の受注処理だけではなく制作フローを通して一貫したデータを
共有することによりスムーズな制作と生産性の向上を図ります。
・新規ユーザーの増加（直感的にわかりやすい UI ）
・リピート率の増加（マイページ充実による再注文のやりやすさ）
・お客様の入力ストレスの低減（決済システムの組み込みによるマイページ内決済）
・手入力によるデータ不備などの発生数の低減（システム導入・連携による一意のデータを共有
・制作フローでの効率的なお客様対応による顧客満足度の向上、対応時間の削減（マイページ）

2 システムの構想／システムの概要

2-1 システムの構想

EC システムのプラットフォームとして EC-CUBE 4系、 ~~WordPress~~ を導入します。
~~業務システムのプラットフォームとして~~ kintone ~~、メールワイズの導入します。~~
~~また、これら~~ 4 ~~システムの必要箇所を連携します。~~

2-2 システムの概要

- EC-CUBE

オープンソースの EC サイト構築パッケージです。

~~・ WordPress~~

~~オープンソースの~~ CMS ~~（コンテンツ管理システム）システムです。~~

~~・ kintone~~

~~業務に合わせたコミュニケーション機能付のシステムが開発が行えるクラウドサービスです。~~

~~・メールワイズ~~

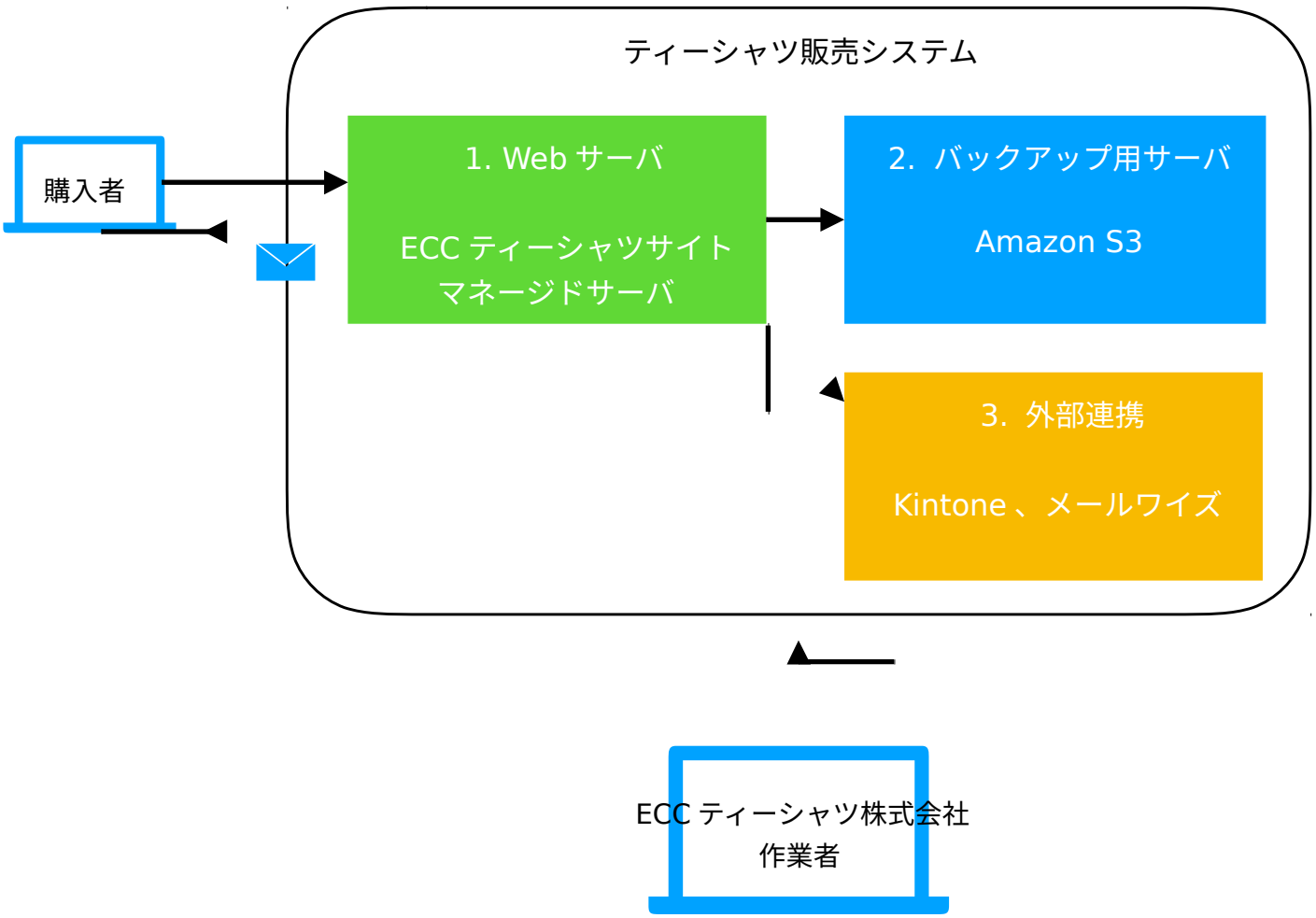
~~共通メールアドレスを複数ユーザーで共有・管理が行えるグループメーラーです。~~

~~2-3 システムへ組み込む項目について~~

~~_受注明細書をベースに項目洗い出し（別途資料｜カテゴリ、選択項目につい~~ 20180830.pdf ~~）~~

2-4 システム構成図

システム構成図



1. Web サーバ ： 公開用サーバ、このサーバに対して EC-CUBE 、 WordPress をインストールする。また、お客様から送信される画像データはこのサーバに保存される。
2. バックアップ用サーバ ： データ保持用サーバ
3. 外部連携サーバ ：kintone やメールワーズなどの他システム

3 機能要求

3-1 機能要求

・ユーザー情報、商品情報、イラスト素材の引き継ぎ

注文データはエクセルにて集計されたもの（同一フォーマット）をベースに引き継ぐ

・注文番号は管理画面側で変更できるようにし、納期・時期によって注文番号を変更させる

・リニューアル後も URL を継承、または 301 リダイレクト

・ TOP ページは WordPress による管理を行い更新性を高める

・管理画面側の権限管理は EC-CUBE 標準のみとする

3-2 EC-CUBE 機能一覧

EC-CUBE の機能として利用するものを以下に挙げます。

そのうち、カスタマイズが必要としている機能には【要カスタマイズ】と記載しています。

https://www.ec-cube.net/product/functionv3.php

※URL としては 3 系であるが、以下の基本機能は 4 系も同様となる

1. フロント機能【要カスタマイズ】
    1.1 TOP ページ
        1.1.1.TOP ページ
    1.2. 商品紹介
        1.2.1. 商品一覧ページ
        1.2.2. 商品詳細ページ
    1.3. 商品お見積もり
        1.3.1. カート
        1.3.2. 商品お見積もり（ログイン / ゲスト購入画面）
        1.3.3. お客様情報
        1.3.4. 商品お見積もり
        1.3.5. お見積り内容確認
        1.3.6. お見積り完了

1.4. 商品注文
1.4.1. カート
1.4.2. 商品購入（ログイン / ゲスト購入画面）
1.4.3. お客様情報
1.4.4. 商品購入 / お届け先の複数指定
1.4.5. ご注文内容確認
1.4.6. 注文完了
1.5. 会員登録
1.5.1. 会員登録
1.5.2. 仮会員登録完了ページ）
1.5.3. 会員登録（完了ページ）
1.5.4. ご利用規約
1.6. マイページ
1.6.1. マイページ TOP
1.6.2. マイページ / 購入履歴詳細
1.6.3. マイページ / 会員情報変更
1.6.4. マイページ / 会員情報登録変更 (完了ページ)
1.6.5. マイページ / 本会員登録 (完了ページ)
1.6.6. マイページ / お届け先追加･変更
1.6.7. マイページ / ログイン
1.6.8. マイページ / 退会手続き (入力ページ)
1.6.9. マイページ / 退会手続き (完了ページ)
1.6.10. マイページ / お気に入り一覧
1.7. その他
1.7.1. パスワード再発行
1.7.2. 当サイトについて
1.7.3. プライバシーポリシー
1.7.4. 特定商取引に関する法律に基づく表記
1.7.5. お問い合わせ (入力ページ)
1.7.6. お問い合わせ (完了ページ)
2. 管理機能
2.1. TOP ページ【要カスタマイズ】
2.1.1. ログイン

2.1.2.TOP ページ
2.2. 商品登録【要カスタマイズ】
2.2.1. 商品マスター
2.2.2. 商品登録
2.2.3. 商品登録 (商品規格)
2.2.4. 規格管理
2.2.5. 規格管理＞分類登録
2.2.6. カテゴリ登録
2.2.7. 商品登録 CSV
2.2.8. カテゴリ登録 CSV
2.2.9. タグ管理
2.3. 受注管理【要カスタマイズ】
2.3.1. 受注一覧
2.3.2. メール通知
2.3.3. メール通知（確認ページ）
2.3.4. 受注登録
2.3.5. 出荷管理
2.3.6. 出荷登録
2.3.7. メール通知
2.3.8. 出荷 CSV 登録
2.4. 会員管理【要カスタマイズ】
2.4.1. 会員マスター
2.4.2. 会員登録
2.5. コンテンツ管理【要カスタマイズ】
2.5.1. 新着情報管理
2.5.2. ファイル管理
2.5.3. ページ管理
2.5.4. レイアウト管理
2.5.5. ブロック管理
2.6. 基本情報設定
2.6.1.SHOP マスター
2.6.2. 特定商取引法
2.6.3. 会員規約設定

2.6.4. 支払方法設定
2.6.5. 支払方法登録編集
2.6.6. 配送方法設定
2.6.7. 配送方法設定
2.6.8. 税率設定
2.6.9. メール管理
2.6.10.CSV 出力項目設定
2.7. システム情報設定
2.7.1. システム情報
2.7.2. メンバー管理
2.7.3. メンバー登録 / 編集
2.7.4. セキュリティ管理
2.7.5. システム情報
2.7.6.EC-CUBE ログ表示
2.7.7. マスターデータ管理

3-3 WordPress 機能一覧

1. WordPress 機能【要カスタマイズ】
1.1TOP ページ
1.1.1.TOP ページ
1.2. お客様の声ページ
1.2.1. お客様の声一覧ページ
1.2.2. お客様の声詳細ページ
1.3. 制作実績ページ
1.3.1. 制作実績一覧ページ
1.3.2. 制作実績詳細ページ
1.4. 新着情報ページ
1.4.1. 新着情報一覧ページ
1.4.2. 新着情報詳細ページ
1.5. 緊急情報ページ
1.5.1. 緊急情報一覧ページ
1.5.2. 緊急情報詳細ページ

3-4 kintone 機能一覧

1. コミュニケーション機能
    1.1. スレッド
    1.2. コメント
    1.3. 個別チャット
2. プロセス管理機能【要カスタマイズ】
    2.1. 承認フロー
3. データベース機能【要カスタマイズ】
    3.1. アプリ
4. データ分析機能【要カスタマイズ】
    4.1. アプリ内データ一覧
    4.2. 集計表・グラフ
5. 通知機能【要カスタマイズ】
    5.1. リマインダー
    5.2. プッシュ通知
    5.3. メール通知

3-5 メールワイズ機能一覧

1. メールアプリケーション
2. 電話履歴 / 訪問履歴
3. アドレス帳
4. テンプレート
5. 一斉送信
6. 集計レポート
7.kintone 連携

4 入力要求と出力要求

4-1 EC-CUBE 入出力要求

1. 入力要求
    1.1.フロント
        1.1.1. 商品の購入
            タオルまたは T シャツの購入
        1.1.2. 会員情報の入力
            会員情報の入力
        1.1.3. 商品情報の入力
            検索時の商品情報入力
    1.2. 管理
        1.2.1. 商品情報の入力
            商品データの登録・編集
            CSV データによる商品登録
        1.2.2. 受注情報の入力
            注文データの登録・編集
        1.2.3. 会員情報の入力
            会員データの登録・編集
        1.2.4. マスターデータの入力
            マスターデータの登録・編集
        1.2.5. 画像などの入力
            画像などのリソースファイルの登録
        1.2.6.kintone からの注文情報データ入力
2. 出力要求
    2.1. フロント
        2.1.1. 商品購入情報の出力
            購入した注文情報を出力
        2.1.2. 会員情報照会
            登録された会員情報の照会
        2.1.3. 商品情報照会
            検索時の商品情報を出力

2.2. 管理

2.2.1. 商品情報の出力

検索条件を元に商品情報の一覧表示

CSV 出力

2.2.2. 受注情報の出力

検索条件を元に受注情報の一覧表示

CSV 出力

帳票出力（マイページ：領収書、管理内：納品書、請求書、 FAX 注文用紙、見積書）

2.2.3. 会員情報の出力

検索条件を元に会員情報の一覧表示

CSV 出力

2.2.4. マスターデータの出力

マスターデータの出力

一部データの CSV 出力

2.2.5.kintone に対する注文情報データ出力

4-2 WordPress 入出力要求

1. 入力要求

1.1. お客様の声

1.1.1. データ取込

1.1.2. データ手入力

1.2. 制作実績

1.2.1. データ取込

1.2.2. データ手入力

1.3. 新着情報の声

1.3.1. データ手入力

1.4. 緊急情報

1.4.1. データ手入力

2. 出力要求

2.1. お客様の声

2.1.1. データ出力

2.2. 制作実績

2.2.1. データ出力

4-3 kintone 入出力要求

1. 入力要求
    1.1. アプリ
        1.1.1.EC-CUBE 自動取込
        1.1.2.CSV 取込
        1.1.3. データ手入力
2. 出力要求
    2.1. アプリ
        2.1.1.CSV 出力
        2.1.2. 帳票出力

4-4 メールワイズ入出力要求

1. 入力要求
    1.1. 受信メール
    1.2. 電話対応履歴
    1.3. メールテンプレート（ kintone アプリ連携）
2. 出力要求
    2.1. 送信メール
    2.2. 集計レポート
    2.3. メール対応履歴（ kintone アプリ連携）

5 システム導入後の業務フロー

_別途資料（全体）｜全体フローとシステム関係 20180824.pdf

別途資料（ kintone/ メールワイズ）｜ kintone_概 20180824.pdf

6 品質・性能要求

- 想定会員数
  - 2018 年 8 月時点 ： 約 25,000 名、
  - 年間会員増加数 ：3,000 件
- 商品数
  - 約 30 件
- 注文件数
  - 1 日 / 200 件、 1 年 / 73,000
- ピーク時同時接続数
  - 1 分間に 5 件の注文が可能
  - 1 分間に 100 人が同時アクセスしてもトップページが表示されること
- メール件数
  - 1 日最大 2,000 件 + α (注文メール、見積もりメール、発送メール)
- ログファイル保存数
  - 半年間ログを保存
- データ転送量 (1 日)
  - トップページ ：1 ページ容量 (3MB) × 10,000PV = 30,000MB(30GB)
  - トップページ以外 ：1 ページ容量 (1MB) × 10,000PV = 10,000MB(10GB)
  - 画像アップロード ：1 日 / 1 画像データ最大 20MB × 1 日最大受注 100 件 = 2GB
  - 合計 ：42GB

7 インフラ設計要求

利用するハードウェアに関してはレンタルサーバあるいは VPS ・クラウドを利用することを想定し、ハードウェアのメーカー、型番、詳細スペックは保証しません。また、運営者が手間をかけることなく運用できることを最優先とします。
（今回は VirtualBox の仮想マシンを使用）

1. ハードウェア構成
   1.1 Web サーバ、 DB サーバ
   Web サーバ、 DB サーバともに同一サーバ内に保持し、サーバの冗長化は行いません。ただし、今後のサービス展開によってオプションにてサーバの冗長化を行います。
   1.2. メールサーバ
   メールサーバはレンタルサーバの場合、同一サーバ内で利用し、 VSP ・クラウドを想定した場合、別途サーバで運用します。
2. ハードウェア費用例
   2.1. レンタルサーバの利用
   2.1.1. **さくらのマネージドサーバ SSD プラン** (https://www.sakura.ne.jp/managedserver/)
   安定性、性能を重視したサーバー 1 台専有プラン
   月額 ：19,440 円、年間一括の場合 ：213,840 円
   初期費用 ：59,400 円
   SSD 容量 ：360GB
   転送量 ：200GB/ 日
   2.2. さくらのマネージドサーバの特徴
   サーバー 1 台を専有し、 CPU やメモリなどを独占でき
   他のサーバー利用者の利用状況によるパフォーマンスへの影響を受けない
   専用サーバーにしたいけど、めんどうな運用はまかせたい
   社内にサーバーに詳しい管理者がいなくても、セキュリティ対策や障害対応、バックアップなど、サーバー構築や運用管理はサーバ会社で管理

3. クライアントブラウザ要件
   3.1. 対応ブラウザ
   3.1.1.Windows
   Internet Explorer11 以降、 Edge 最新版、 Chrome 最新版、 Firefox 最新版
   3.1.2.Mac

Safari 最新版、 Chrome 最新版、 Firefox 最新版

3.1.3.iOS(11 以降)

Safari 最新版

3.1.4.Android(6 以降)

標準ブラウザ最新版、但し、 Android6 系に関して一部機種は非対応

8 アプリケーションセキュリティ要求

本ドキュメントでは Web システム /Web アプリケーションに関して一般的に盛り込むべきだと考えられるセキュリティ要件について記載しています。ただし、ネットワークやホストレベル、運用などに関するセキュリティ要件については記載していません。
セキュリティチェックについては The Open Web Application Security Project (OWASP) と呼ばれるフリーツールを利用して確認を行います。 (https://www.owasp.org/)

以下のセキュリティ要求を満たすために OWASP を利用します。

1. 認証
    1.1以下の箇所では、ユーザー認証を実施すること
        1.1.1. 特定のユーザーのみに表示・実行を許可すべき画面や機能
        1.1.2. 上記画面や機能に含まれる画像やファイルなどの個別のコンテンツ (非公開にすべきデータは直接 URL で指定できる公開ディレクトリに配置しない)
        1.1.3. 管理者用画面
    1.2. パスワードについて
        1.2.1. パスワード文字列は少なくとも大小英字と数字の両方を含み、最低 8 文字以上であること
        1.2.2. パスワード文字列の入力フォームは input type="password" で指定すること
        1.2.3. ユーザーが入力したパスワード文字列を次画面以降で表示しないこと
        1.2.4. パスワード文字列は「パスワード文字列 +salt(ユーザー毎に異なるランダムな文字列) 」をハッシュ化したものと salt のみを保存すること (salt は 20 文字以上であることが望ましい)
    1.3. パスワードリセット機能について
        1.3.1. パスワードリセットを実行する際にはユーザー本人しか受け取れない連絡先 (あらかじめ登録しているメールアドレス、住所、電話番号など) に再設定方法を通知すること
        1.3.2. パスワードはユーザー自身に再設定させること
2. セッション管理
    2.1. セッションの破棄について
        2.1.1. 認証済みのセッションが一定時間以上アイドル状態にあるときはセッションタイムアウトとし、サーバー側でセッションを破棄しログアウトすること

2.1.2. ログアウト機能を用意し、ログアウト実行時にはサーバー側でセッションを破棄すること

2.2. セッション ID について

2.2.1.Web アプリケーション開発ツールが提供するセッション管理機能を使用すること

2.3.CSRF(クロスサイトリクエストフォージェリー) 対策の実施について

2.3.1. ユーザーにとって重要な処理を行う箇所では、ユーザー本人の意図したリクエストであることを確認できるようにすること

3. パラメーター

3.1. URL パラメーターにユーザー ID やパスワードなどの秘密情報を格納しないこと

3.2. パラメーターにパス名を含めないこと

3.3. 入力値の文字種や文字列長の検証を行うこと

4. 出力処理

4.1. HTML として特殊な意味を持つ記号 (< > " ' &) を文字参照によりエスケープすること

4.2. 外部から入力した URL を出力するときは「 http:// 」または「 https:// 」で始まるもののみを許可すること

4.3.HTTP レスポンスヘッダーの Content-Type を適切に指定すること

4.4.HTTP レスポンスヘッダーフィールドの生成時に改行コードが入らないようにすること

4.5.SQL 文を組み立てる際に静的プレースホルダを使用すること (SQL インジェクションの回避)

4.6. プログラム上で OS コマンドやアプリケーションなどのコマンド、シェル、 eval() などによるコマンドの 実行を呼び出して使用しないこと

4.7. リダイレクタを使用する場合には特定の URL のみに遷移できるようにすること

4.8. レスポンスヘッダーに X-Frame-Options を指定すること

5. HTTPS

5.1. 重要な情報を扱う画面や機能は HTTPS で保護すること

5.2. サーバー証明書はアクセス時に警告が出ないものを使用すること

5.3. 安全な暗号化通信を使用すること

5.3.1.TLS1.0 以上を使用し、 SSL2.0/3.0 を無効にすること

6. cookie

6.1. cookie の属性を適切に設定すること

6.1.1.HTTPS 利用時には Secure 属性を付けること

6.1.2.HttpOnly 属性を付けること

7. その他

7.1. 鍵や秘密情報などに使用する乱数的性質を持つ値を必要とする場合には、暗号学的な強度を持った疑似 乱数生成系を使用すること

7.2. 公開ディレクトリには公開を前提としたファイルのみ配置すること

7.3. 重要な処理が行われたらログを記録すること

アプリケーションセキュリティ参考文献

「 Web システム／ Web アプリケーションセキュリティ要件書 2.0 」

(https://github.com/ueno1000/secreq)

9 OS/ ミドルウェアに関するセキュリティ条件

OS 、及びミドルウェアのパッチ適用に関してはサーバ会社管理となるため、今回は特に行いません。アプリケーションで利用しているミドルウェアに関しては脆弱性などが発見され次第対応します。

10 運用

- 利用時間 ：365 日 24 時間運用。
- データ保持期間 ： マスターデータ、トランザクションデータの保持期間は全量保持
- パックアップデータ保持期間 ： 半年を想定

11 バックアップ要件

システム障害時にバックアップデータから復旧できるように Amazon S3 へシステム情報 (Web アプリケーション全体、データベース情報) を保存する。保存するタイミングは日次とし、仮に障害が発生してバックアップデータから復旧する場合、日次で保存されたデータからとする。

- 主なデータ容量予測
    - Web アプリケーション全体 (EC-CUBE 、 WordPress)
        - EC-CUBE 全体 ：1 日 / 500 MB
        - WordPress 全体 ：1 日 / 100MB
        - 受注時の画像 ：1 日 / 1 画像データ最大 20MB × 1 日最大受注 200 件 = 4GB
        - 合計 ：1 日 / 4.6GB 、 1 ヶ月 / 138GB
    - データベース (EC-CUBE 、 WordPress)
        - 1 日 / 300MB 、 1 ヶ月 / 9GB
- バックアップデータ保持期間
    - 半年間データを保持

- 1 ヶ月の AmazonS3 へのデータ容量・金額
    - 保存時に必要な最大データ容量 ：(138GB + 9GB) × 6 ヶ月 = 882GB
    - S3 金額 ：882GB × 0.025USD/GB = 22.05 USD/ 月 (約 2,400 円 〜 2,600 円)

参考 ：https://aws.amazon.com/jp/s3/pricing/

12 保守

- 構築に当たっては十分なセキュリティ対策を講じ、情報漏えい対策が十分に講じる
- 異常又は障害が発見された際には、直ちにユタカさまへ連絡し、復旧手段について万全を期す
- 障害発生時には、原因を調査の上、報告書を提出
- 受付時間 :10 時〜 17 時

13 参考資料

- _概算スケジュー_ 20180830.pdf
- _ランニング費_ 20180830.pdf
- 管理画面の各機能とフロントサイトとの関連性 .pdf
- EC システム・業務システム質問表（ Google スプレッドシート）
- 業務管理ファイル一覧（ Google スプレッドシート）