

診断項目一覧(サンプル)

No	カテゴリ	重要度	指摘箇所	想定されるリスク・懸念点	推奨される対策	備考
1	メンテナンス性	A	ヘッダー・フッターのHTMLがテンプレート(themes/custom/annai/include/footer.html.twig, themes/custom/annai/include/header.html.twig)に直接埋め込まれています。	本来であればテーマでリージョンだけ切り、UIからブロックなどを配置しレイアウトを行うべきです。 現状の作りでは、管理UIからヘッダー、フッターを変更できず、都度ソースコードの変更が必要になります。	ヘッダー、フッターをクライアントが編集できるようにするかどうかで工数が大きく変わりますが、通常弊社では仕様決定の際にご提案しております。御社のサイト構造から鑑みるにこれは必須事項かと思われます。 例: 製品情報の各スイート以下の文言やメニュー項目などのお客様による変更 Drupalのブロック、メニュー機能を使い、サイト管理者がDrupalの管理UI上から変更できるように実装し直すことを推奨します。	
2	メンテナンス性	A	・ケーススタディ用のTwigテンプレート内でclass名がコンテンツに依存する実装になっています。 ・クライアントページのサブタイトルやサイドバーがテンプレート内で実装されています。	この実装ではタイトルが変わった場合などにclassが変わり、スタイルが当たらなくなる可能性があります。 また、テンプレート内のリンクとして、URLがハードコーディングされているため、UIからコントロールすることが不可能です。	コンテンツの内容や入力項目など、動的に変化する値に依存する実装は避けるべきです。	
3	メンテナンス性	A	themes/custom/annai/css/ 以下のcssファイルが、Drupalの動的コンテンツ用ディレクトリ (sites/default/files)内の画像ファイルを参照しています。	動的コンテンツ用のディレクトリはgitによるバージョン管理の対象外となっているため、今のファイル配置ではテーマの動作がソースコードで保証されません。	cssが参照する背景等の画像は動的コンテンツ用のディレクトリではなく、テーマのディレクトリ内に移動し、gitによるバージョン管理の対象としてください。	
4	メンテナンス性	A	ノードID毎に個別のテンプレートを作成している (themes/custom/annai/templates/node--8.html.twigなど)	既存のパスを別のノードで置き換えた場合に正しく動作しません。 例えば、現在 /news は node/8 (node id = 8)のノードのエイリアスです。 Drupalのnaming conventionにより、このページには node--8.html.twig が利用されます。 将来的にこのページを作り直すなどでノードIDが変わると今のテンプレートは適用されなくなるため、新しいテンプレートファイルの作成も必要になります。	ノードID毎に個別にテンプレートを定義する必要があるように、デザインの仕様を調整することを推奨します。	
5	メンテナンス性	A	テーマで上書きされているテンプレートファイルが49個あり、多くのファイルにリンクなどがハードコーディングされています。	今の作りでは、些細なデザインの変更だけでもテンプレートファイルの書き換えが必要になり、サイトの運営上利便性を損なう可能性があります。	DrupalコアのViewsの設定変更やブロック等で置き換え可能な部分は、テンプレートファイルを使わずに実装することを推奨します。	
6	メンテナンス性	A	ニュースと導入事例のパンくずリストの上位階層がテンプレートにハードコーディングされています。	URLやデザインが変更されたときに追従できない作りになっています。	easy_breadcrumbなどのモジュールを導入することを推奨します。	
7	メンテナンス性	A	古いjQuery (1.10.2)が挿入されています。	Drupal 8.5.1はjQuery v3.2.1を利用しています。古いjQueryが挿入されることによって予期しない動作を引き起こす可能性があります。 現状のサイトではログインすると、ほぼ全てのページでJavaScriptのエラーが発生します。 また、未ログイン状態でも /news でJavaScriptのエラーが発生することを確認しています。 更に設定不足の部分もあり作成者の想定外のページではページが乱れる原因にもなっています。 この実装にはいくつかの問題があります。 1. ヘッダー、フッターなどがページ全体がHTMLファイルとして管理されているため、Drupal側のサイトの設定変更と連動しません。 2. メールの宛先、文面等全てがHTMLファイル内に直接コーディングされており、変更の際にファイルの更新が必要になります。 3. CSRFトークン等の連続したアクセスを抑制する仕組みがないため、簡単に外部からサーバーに負荷を与える攻撃が可能です。CSRFについては https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/301.html を参照してください。	テーマのJavaScript全体を古いjQueryに依存しないように書き直すことを推奨します。	
8	セキュリティ	A	問い合わせフォームがDrupalではなくstaticなHTMLとphpファイルで実装されています。		問い合わせフォームについては、coreに含まれるcontact formモジュールか、webformモジュールを利用することを推奨します。	
9	メンテナンス性	A	テーマのJS、CSSを利用せずに、Asset Injectorモジュールで大量のcss.jsが挿入されています。 https://www.drupal.org/project/asset_injector	CSSなどのアセットは通常サイト内で共通のため、テーマ内に格納するのが常でありルールでもあります。 また、コンテンツタイプによってはコンテンツのpathが変更されるとスタイルが当たらなくなる可能性もあります。 更に設定不足の部分もあり、作成者の想定外のページではページが乱れる原因にもなっています。 Asset Injectorではパスと挿入するアセットを組みで管理するため、コンテンツのパスが変わった場合に、合わせて設定を変更する必要があります。 また、Asset Injectorに設定したコードはDB内に保存され、gitでバージョン管理されないため、テーマの動作がソースコードで保証されません。	Asset Injectorの利用はゼロもしくは最小限にすべきです。(弊社では利用自体を推奨しません) css.jsなどのアセットは基本的にはテーマのアセットとして管理し、gitでバージョン管理すべきです。必要なファイルを適切にassetとして管理してください。 詳しくは https://www.drupal.org/docs/8/theming-drupal-8/adding-stylesheets-css-and-javascript-js-to-a-drupal-8-theme をご参照ください。	
10	セキュリティ	B	uid=1のデフォルトユーザー(admin)が有効になっています。	このユーザーは全ての権限設定をバイパスする特殊なユーザーです。 詳しくは https://www.drupal.org/node/947312 をご参照ください。	Drupalコアのアップデートなど、特殊な操作をする時以外はuid=1のユーザーはブロック状態にし、通常の運用では利用しないことを推奨します。	
11	メンテナンス性	B	サイトの機能として必要のないモジュールが有効になっています。 (ctools, comment, contact, devel, workflowなど)	ctoolsのcontributeモジュールはDrupalコアのバージョンアップにすぐに対応しないことがあり、アップデートに失敗する可能性がありますがある。	機能として利用していないモジュールは、コアかcontributeモジュールかに関わらず、全てアンインストールすることを推奨します。 コントリビュートモジュールについてはアンインストールに加え、ソースコードも削除してください。	
12	パフォーマンス	C	page cacheが有効化されていません。	キャッシュが有効に利用されず、サーバーの負荷が高くなる、ページの表示に時間がかかるなどの問題が発生する場合があります。	ページにユーザー固有の要素を含まないのであれば、 /admin/config/development/performance で page cacheを有効にしてください。 外部のキャッシュ機構を併用している場合は、この対応は必須ではありません。	
13	ガバナンス	C	サイトの運営がadministratorロールを持つユーザーのみで構成されています。	サイト全体の変更が可能なアカウントでコンテンツの作成や編集を行うことになるため、操作ミスなどでサイトに不具合が生じるリスクが高くなります。	運用次第ですが、administratorユーザーでコンテンツの作成、編集などを行うことは推奨しません。 サイト管理者、コンテンツ編集者など適切なロールを設定し、通常のコンテンツ作成、編集には限定した権限を持つアカウントを利用することを推奨します。	
14	メンテナンス性	C	テーマに含まれる全てのcssファイルがDrupalのコーディングスタンダードに準拠していません。	準拠されていない内容についてはphpcs_drupal.txt をご参照ください。	Drupalのコーディングスタンダードに準拠するようにフォーマットを修正してください。	
15	メンテナンス性	C	twig_tweakモジュールが安定版ではありません。 https://www.drupal.org/project/twig_tweak	twig_tweak 8.x-2.0-rc4 が使われていますが、これは安定版ではなく、Drupal.orgのセキュリティメンテナンスの対象外となっています。	安定版である 8.x-1.9 を利用することを推奨します。 影響範囲を調査し、可能であれば8.x-1.9にダウングレードしてください。 可能であれば、twig_tweakを利用せずにテーマを実装すべきです。	
16	不具合	B	faviconが設定されていません。	サイトにアクセスしたときにfaviconが表示されません。	theme/custom/annai/favicon.png がfaviconとして認識されるようにテーマを適切に修正してください。	
17	メンテナンス性	C	ソースコードがバージョン管理されていません。	コードに何らかの形で意図しない変更がされた場合に検知が困難になる。 過去のコード上の変更履歴を参照できないため、不具合発生時に問題の究明が困難になる。	GITなどのバージョン管理システムを導入してください。	