espar

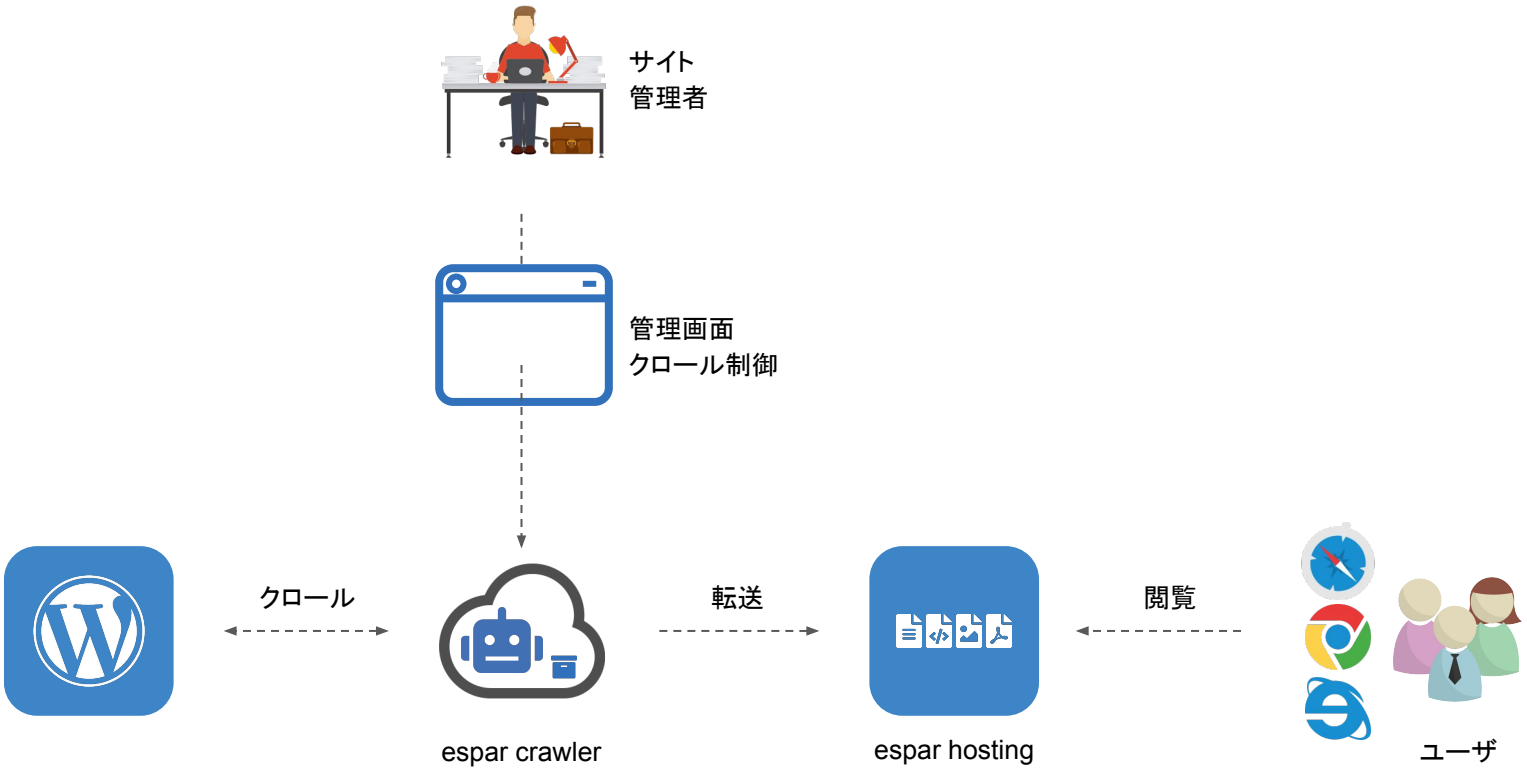
制作会社様向け技術資料

rev.201903

Table of contents

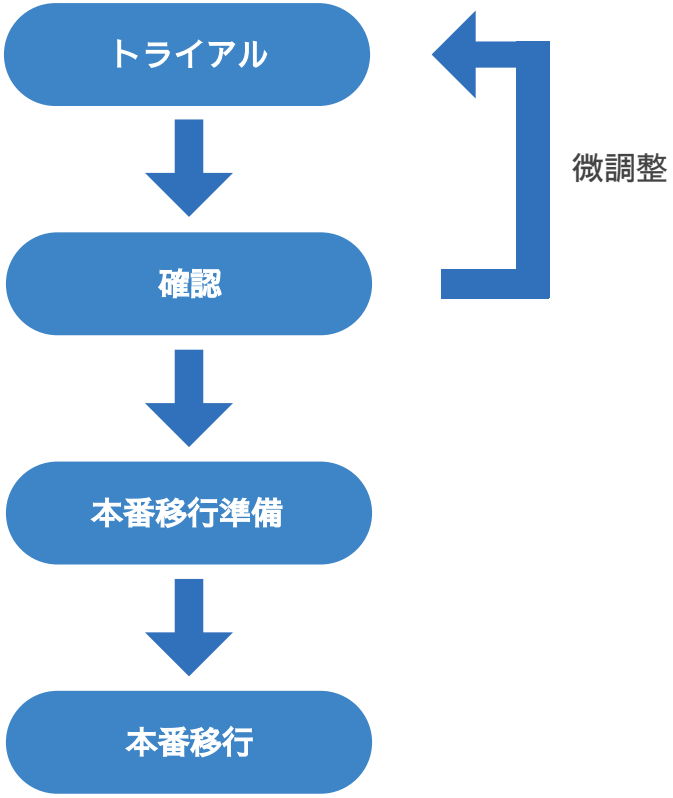
Table of contents

Basic architecture



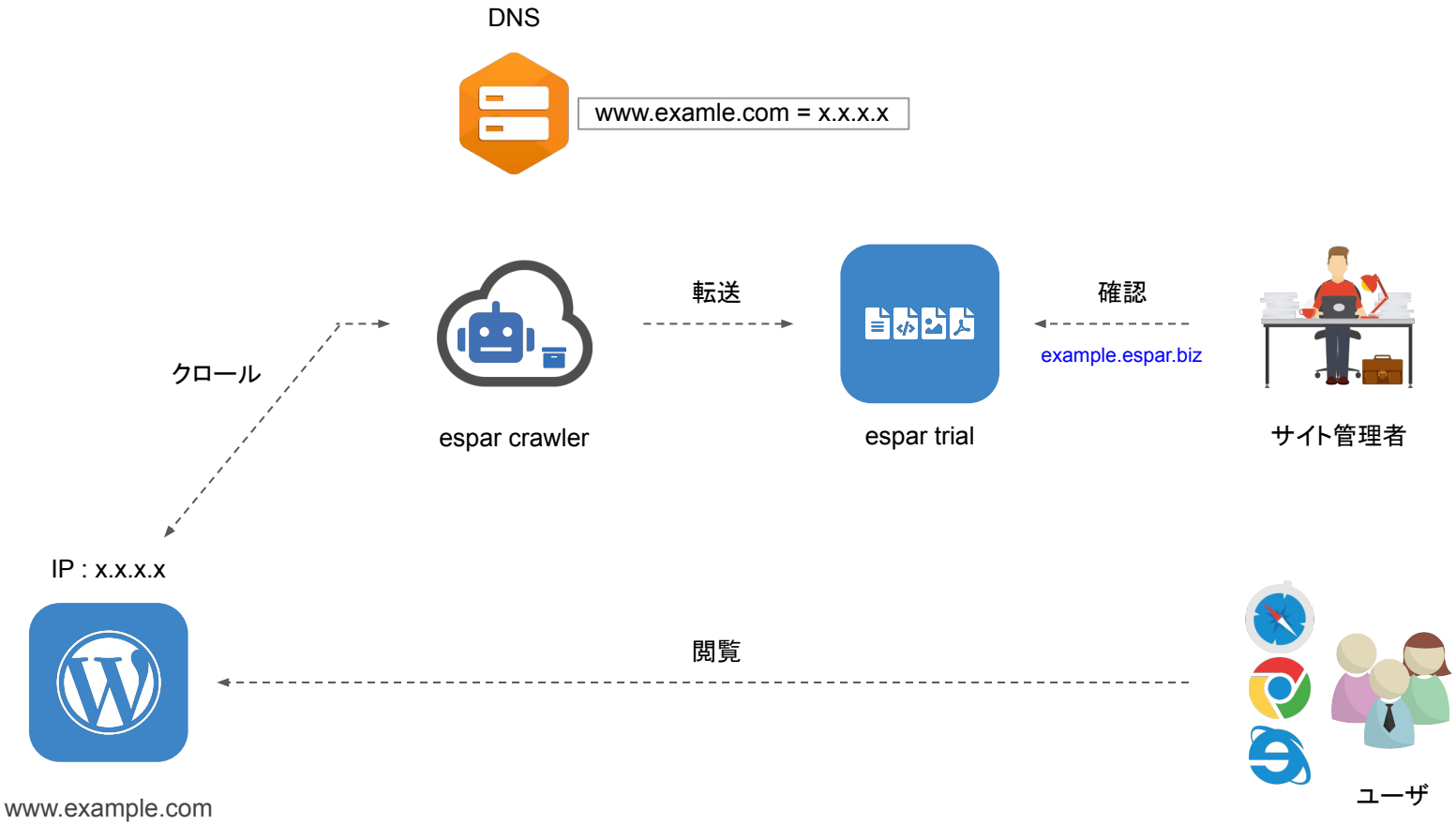
espar導入後は、「サイト公開」の役割は espar hosting が担うようになります。

Process



espar の導入に当たり、まず当社でトライアル環境を構築します。静的化によるサイトの再現ができているかどうかを御確認を頂いたのち、本番移行となります。

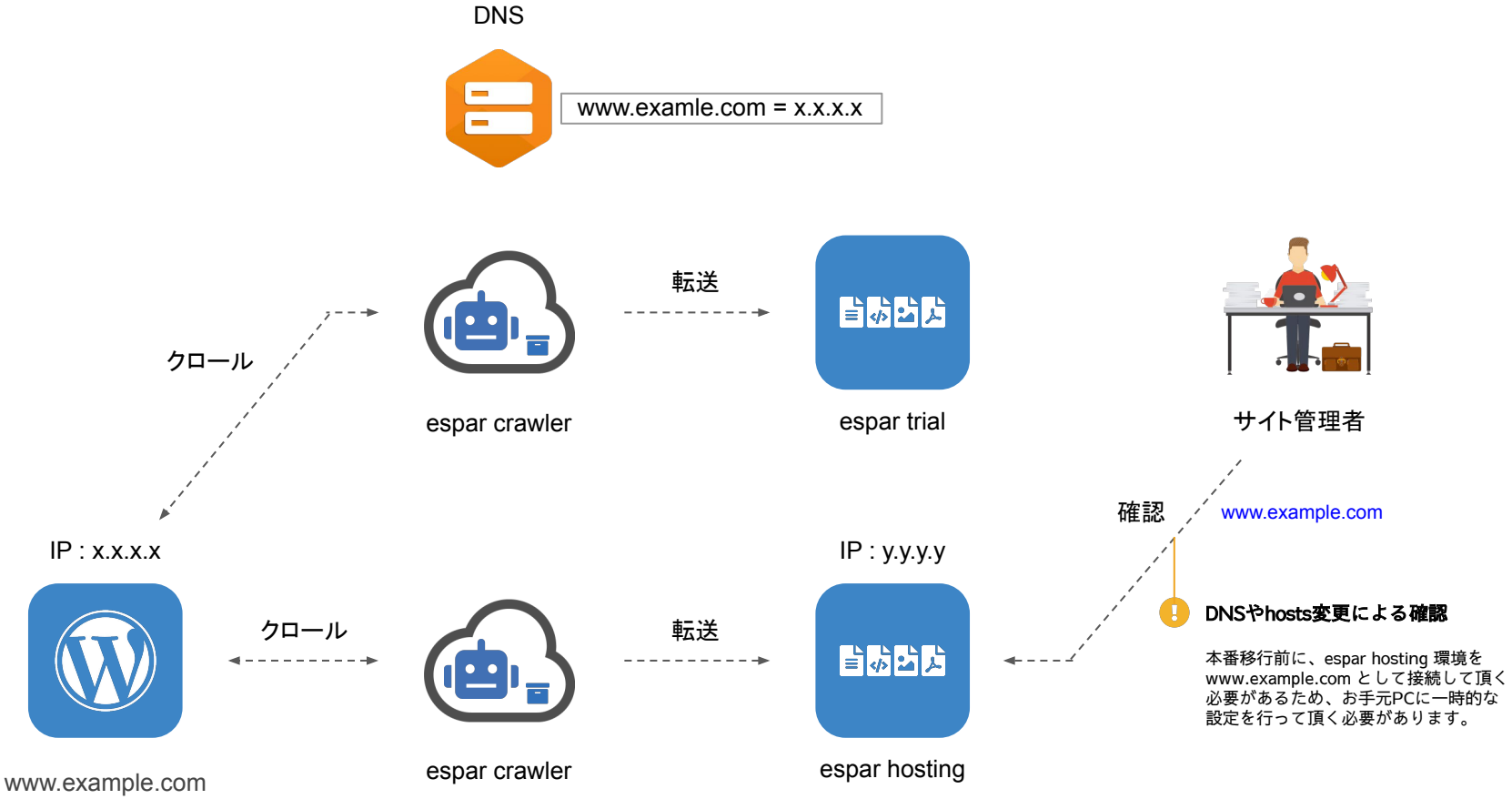
Trial



WordPressサイト (ホスト名を www.example.com とする) を espar crawler でクロールし、確認用のトライアル環境を構築します。トライアル環境には サイト識別子.espar.biz というホスト名を割り当てます。

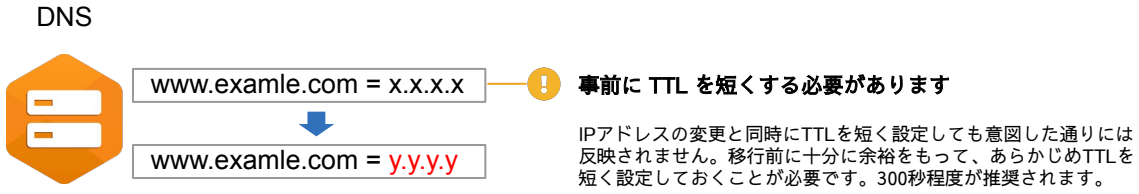
この間、ユーザは従来と変わらず WordPress サーバを直接参照しています。

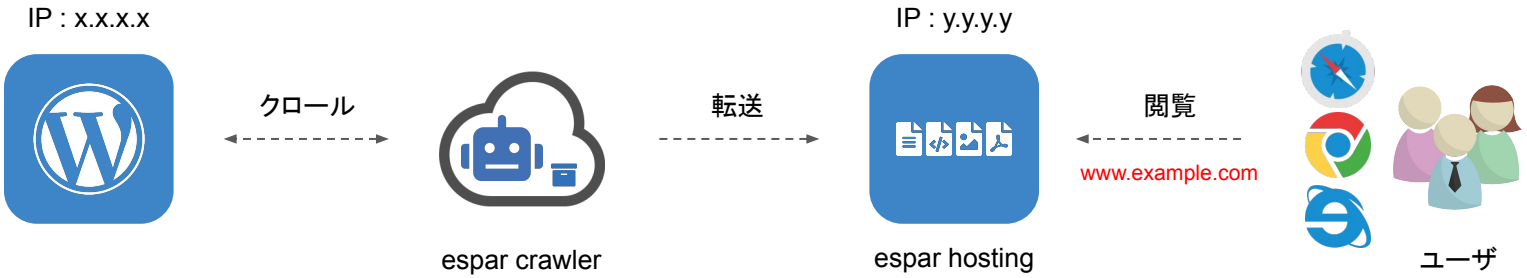
Preparing



トライアル環境で正常に静的化ができていることを確認できれば、本番移行の準備を行います。当社で公開用ホスティングサーバ (espar hosting) に同じ設定で環境構築します。完了後、公開用ホスティングサーバを www.example.com として接続し最終確認を行って頂きます。

Transition

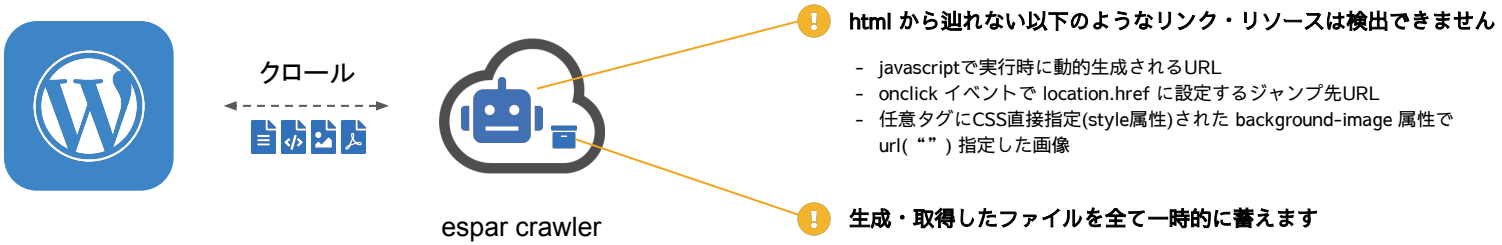




本番移行時は、DNSレコードを espar hosting 側に変更することのみです。DNS変更後、閲覧用のアクセスが WordPressサーバ側に直接届くことはなくなります。

Table of contents

Crawling

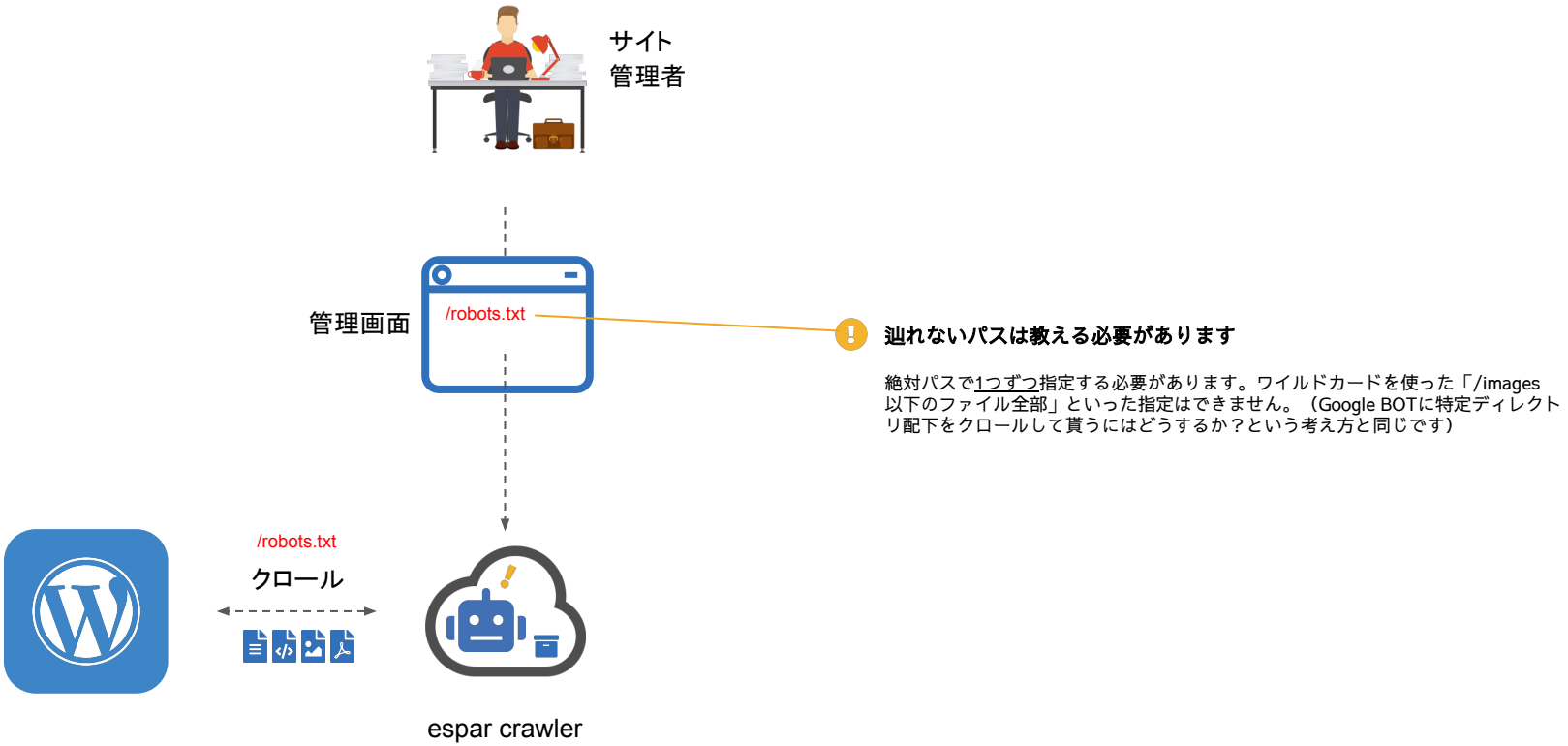


espar crawler は、WP サイトの外部から WP にアクセスする Web サイトクローラーです。(Google BOTのようなもの)

サイトのTOPページをスタート地点にして、 html 中の a タグを頼りにサイト内の全リンクを解析し、全ページ html ファイル化していきます。同時に html から参照されているリソース (画像, 動画, 音声, CSS, PDF, JS 等) も取得します。html の DOM 構造内に記述が現れないページやリソースは取得対象になりません。

espar crawler は生成した html や取得したリソースファイルを、クロールが終了するまで保持します。

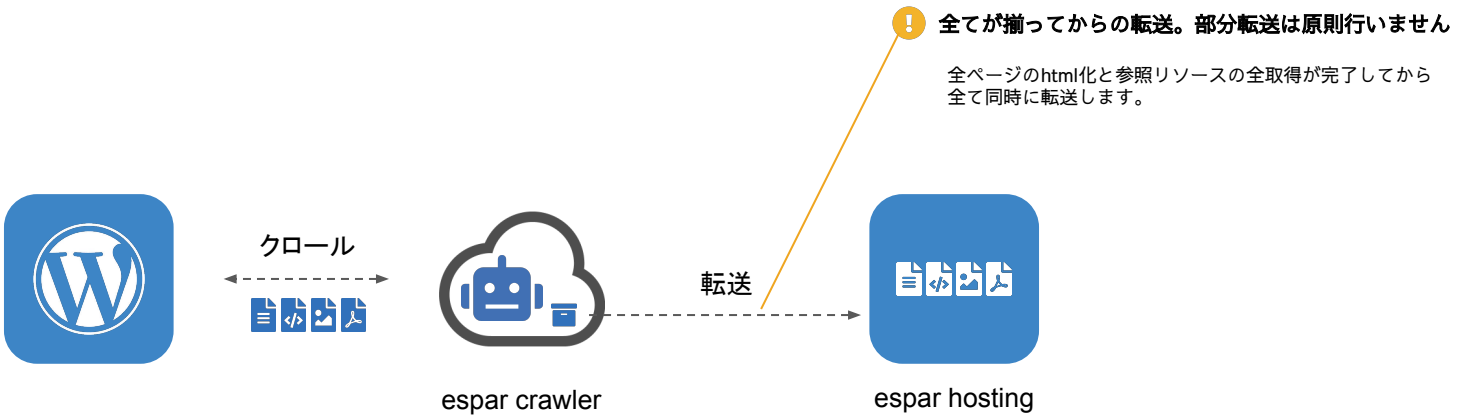
Crawling



TOP からの html リンクでは辿り着けないがサイト公開に必要なファイルが存在する場合、 管理画面で当該 URL を「追加パスとして指定」します。espar crawler は追加パスの指定に従いファイルを明示的に取得しにいきます。例えば、以下のようなファイルが対象となります。

- robots.txt
- sitemap.xml
- Google SearchConsole や facebook 広告の初期設定時に必要なドメイン認証用htmlファイル

Transfer



クロールを全て終えたあと、espar crawler は一時保管した内容を公開用ホスティングサーバ (espar hosting) に転送します。

Table of contents

can’t directly access

サイト管理者

ssh / ftp

公開側への直接接続・操作は一切できません

Webセキュリティ事故の大半は「公開の役割を担う領域」に容易にアクセスできるようにしていることが原因です。

クロール

転送

espar crawler

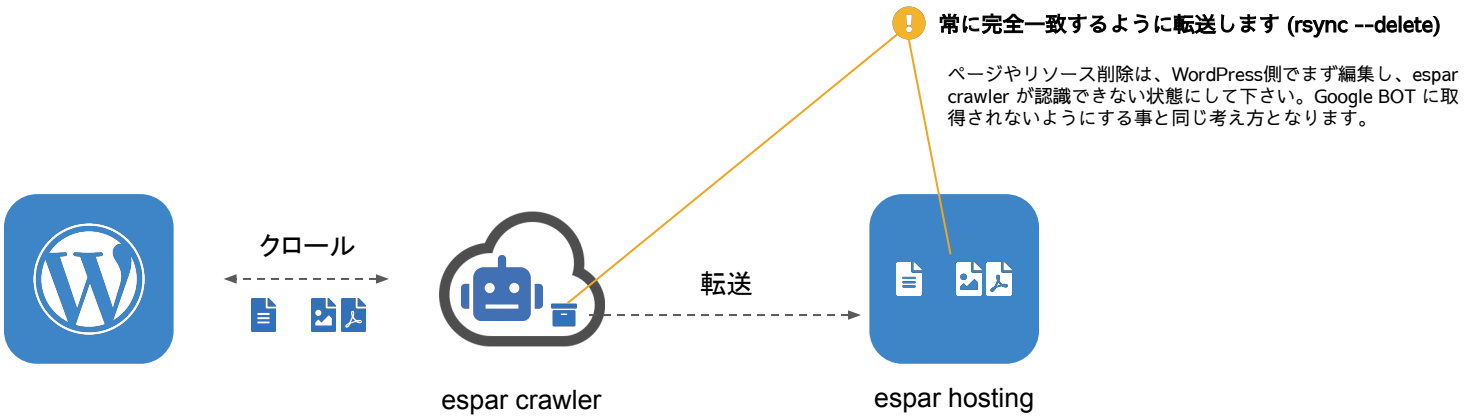
espar hosting

必要最低限のポートのみOPEN

外向きには80, 443番ポートのみOPENしています。内向きには ssh のみOPENしており、root権限使用不可・パスワード認証不可・接続元IP制限などの条件があります。

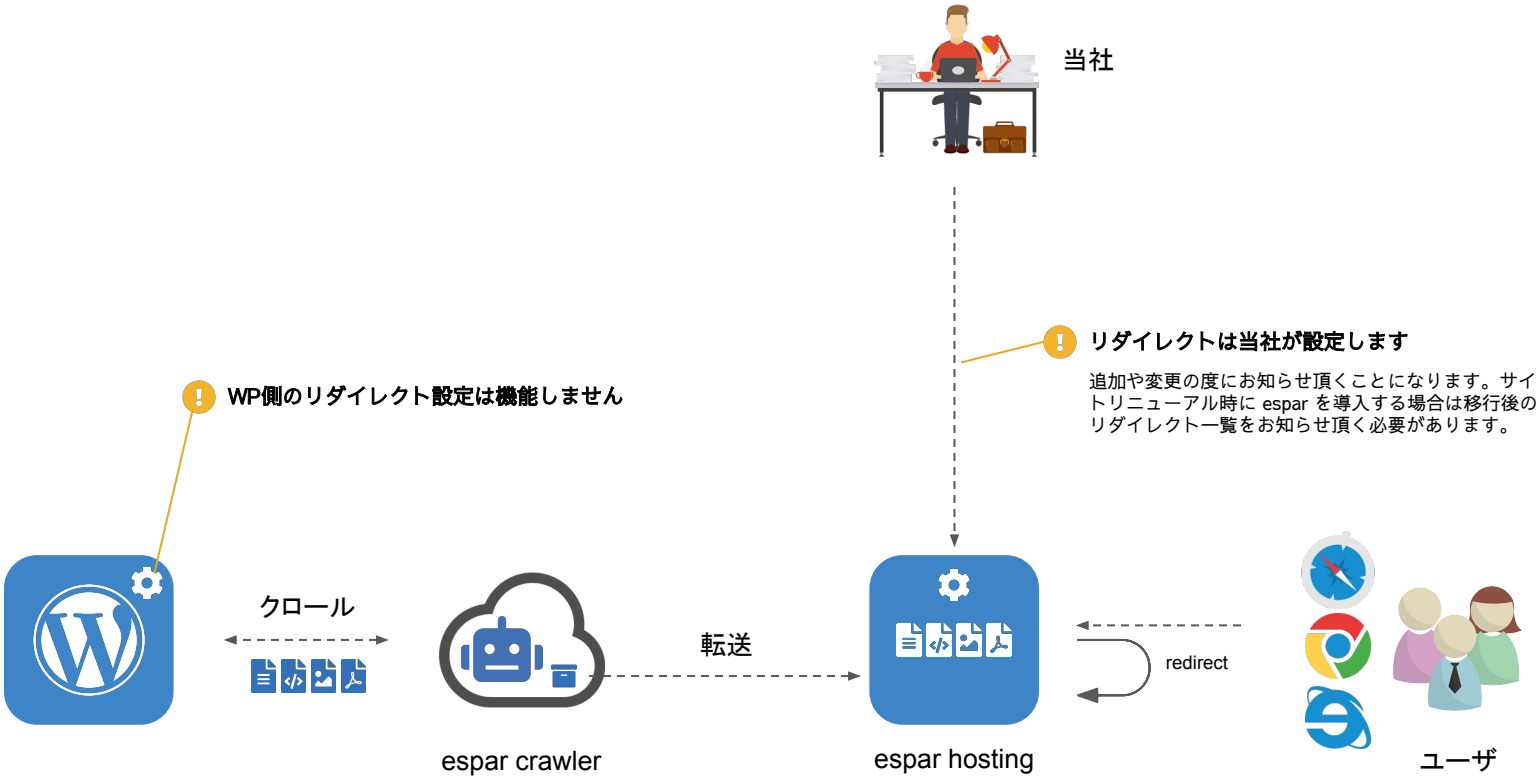
セキュリティ対策のため、espar hosting は「deny all, each allow」の原則（全てのアクセスを一度拒否し必要最低限のみを許可する）で設定を行っています。直接 ssh や ftp で接続して頂くことはできません。

Deletion



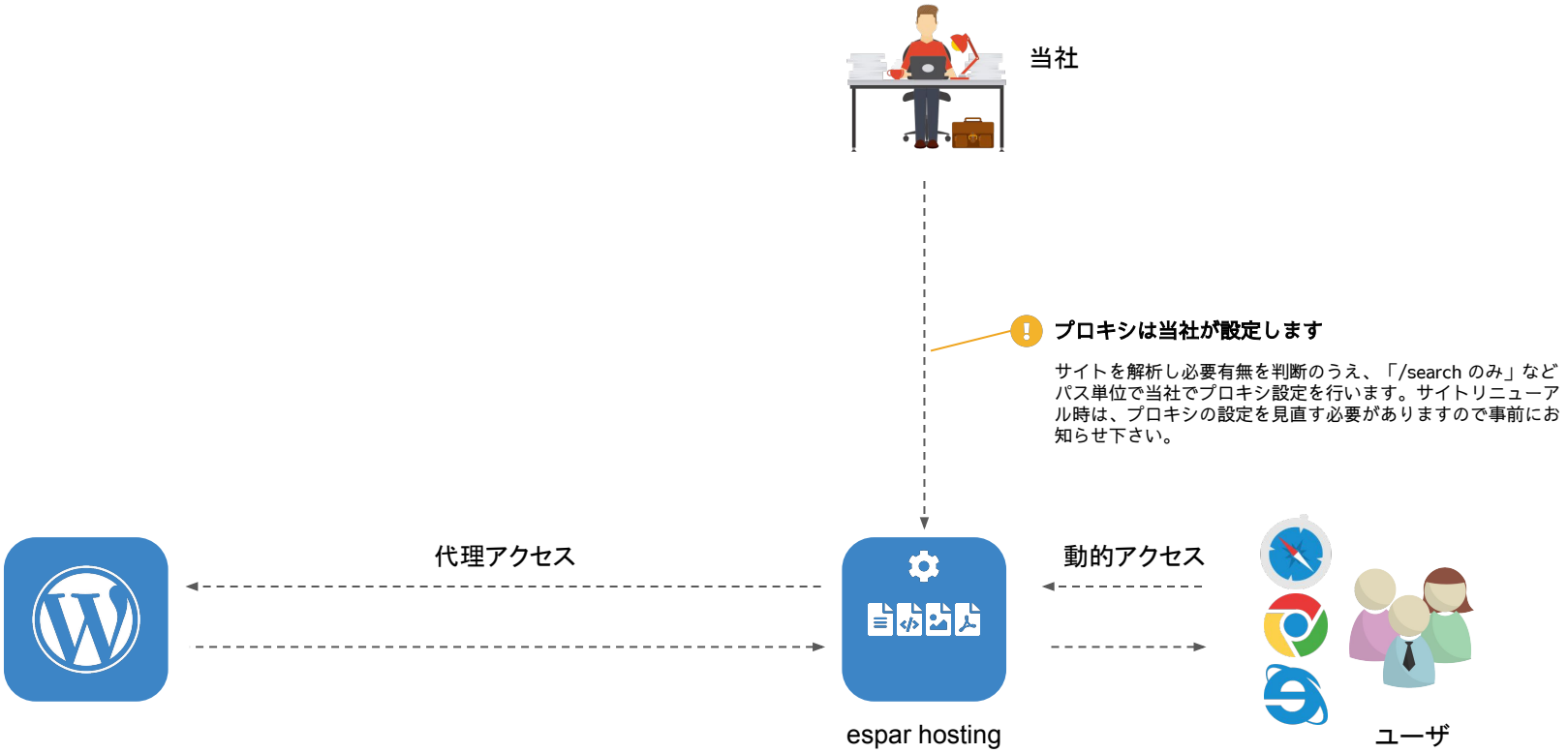
一度公開したページを削除したい場合は、当該ページへのサイト内リンクが現れないようにWordPress側を編集し、そののち再度全体をクロールします。つまり、削除したいものを espar crawler が認識できないように WordPress 側を編集した上で、全体を再クロールする必要があります。

Redirect



リダイレクトの設定は全て公開用ホスティングサーバ (espar hosting) 側で当社が行います。WordPress サーバ側でリダイレクト用プラグインを使用したり、リダイレクト設定を直接行っても反映はされません。(ユーザのアクセスがWordPress側には届かないため)

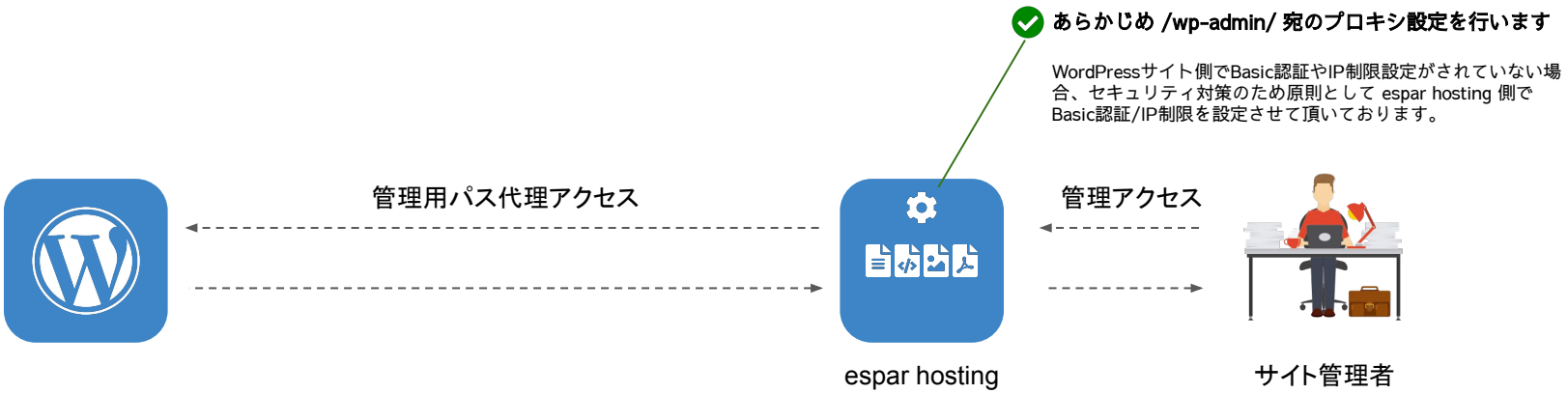
Proxy



サイト内検索など WordPress に直接アクセスする必要がある場合、当該アクセスに限ってユーザに代わり espar hosting が WordPress 本体にアクセスし、取得内容をそのままユーザに返すプロキシ (代理アクセス) を行います。ユーザが直接 WordPress サーバにアクセスすることはありません。

プロキシは WordPress への直接アクセスを許容する仕組みであるため、できるだけ無くすことが推奨されます。(フォームを静的ページで実現する仕組みを採用したり、外部サービスを使用するなど)

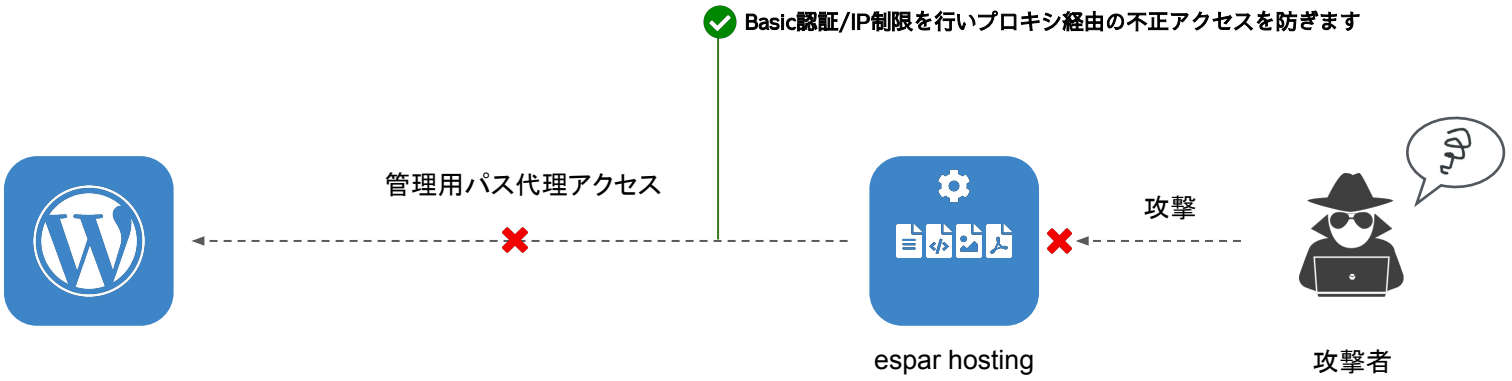
Admin



/wp-admin/ など WordPress の管理画面アクセスにもプロキシ（代理アクセス）を使用します。ただし、管理画面にはサイト管理者のみがアクセスできるよう、espar hosting で IP アドレス制限や Basic 認証を設定します。

Table of contents

Preventing attack



espar hosting には、静的なファイルのみが存在します。データベース・フレームワーク・サーバサイドスクリプト言語 (perl, php, ruby...etc) などは存在しません。よって、悪意ある第三者からの http/https 通信による攻撃はすべて無効化されます。(espar hosting は全て 404 エラーで応答します)

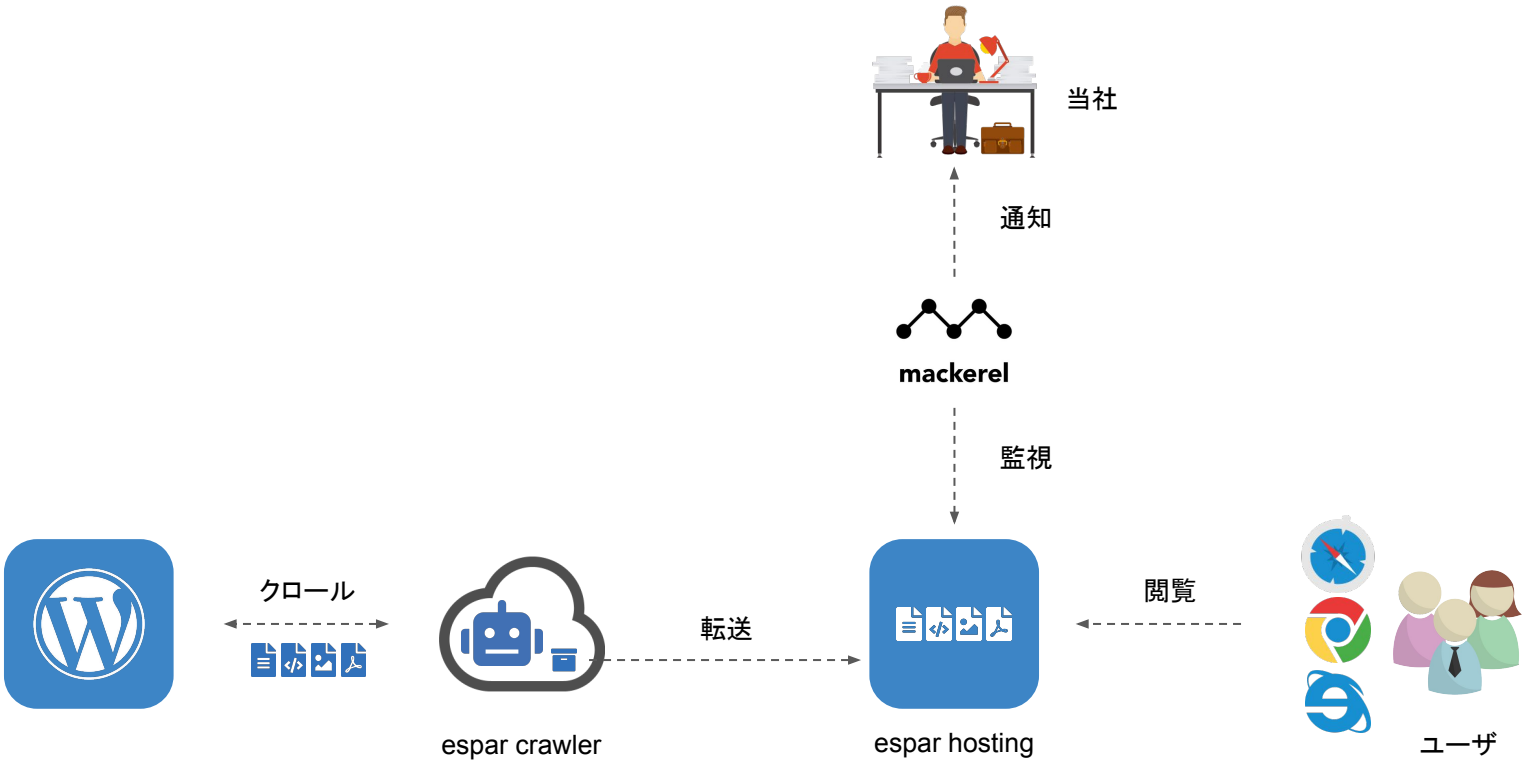
また管理画面へのアクセスにはプロキシ設定がされていますが、 espar hosting 側で Basic 認証や IP アドレス制限が施されており、悪意ある第三者は管理画面にアクセスすることができません。

Hide admin URL

新規サイトの場合は、WordPress 側に公開ホスト名と異なる別ホスト名を設定することが推奨されます。さらに、Basic 認証と IP アドレス制限をかけることで関係者以外が WordPress 側にアクセスできない構成とすることができます。（サイト管理者と espar crawler のアクセスのみ許可）

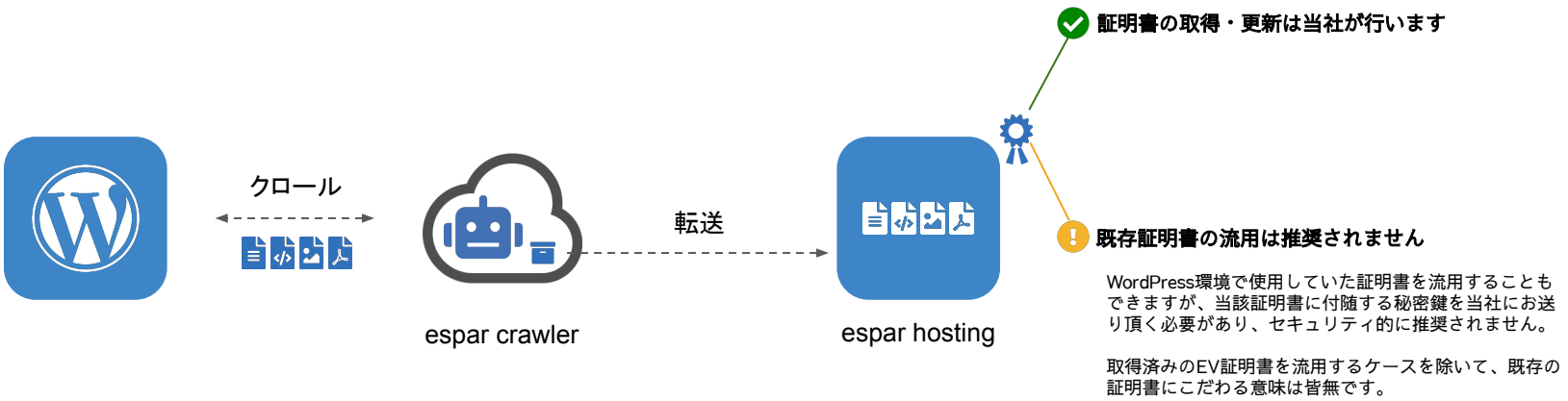
本構成により、第三者による不正なアクセスを理論上全て無効化することができます。悪意ある攻撃者には www.example.com が WordPress で作られたサイトに見えますが、関係者が情報を漏えいしない限り本当の WordPress サーバがどこに存在するか分からず、辿り着くことができません。

Monitoring



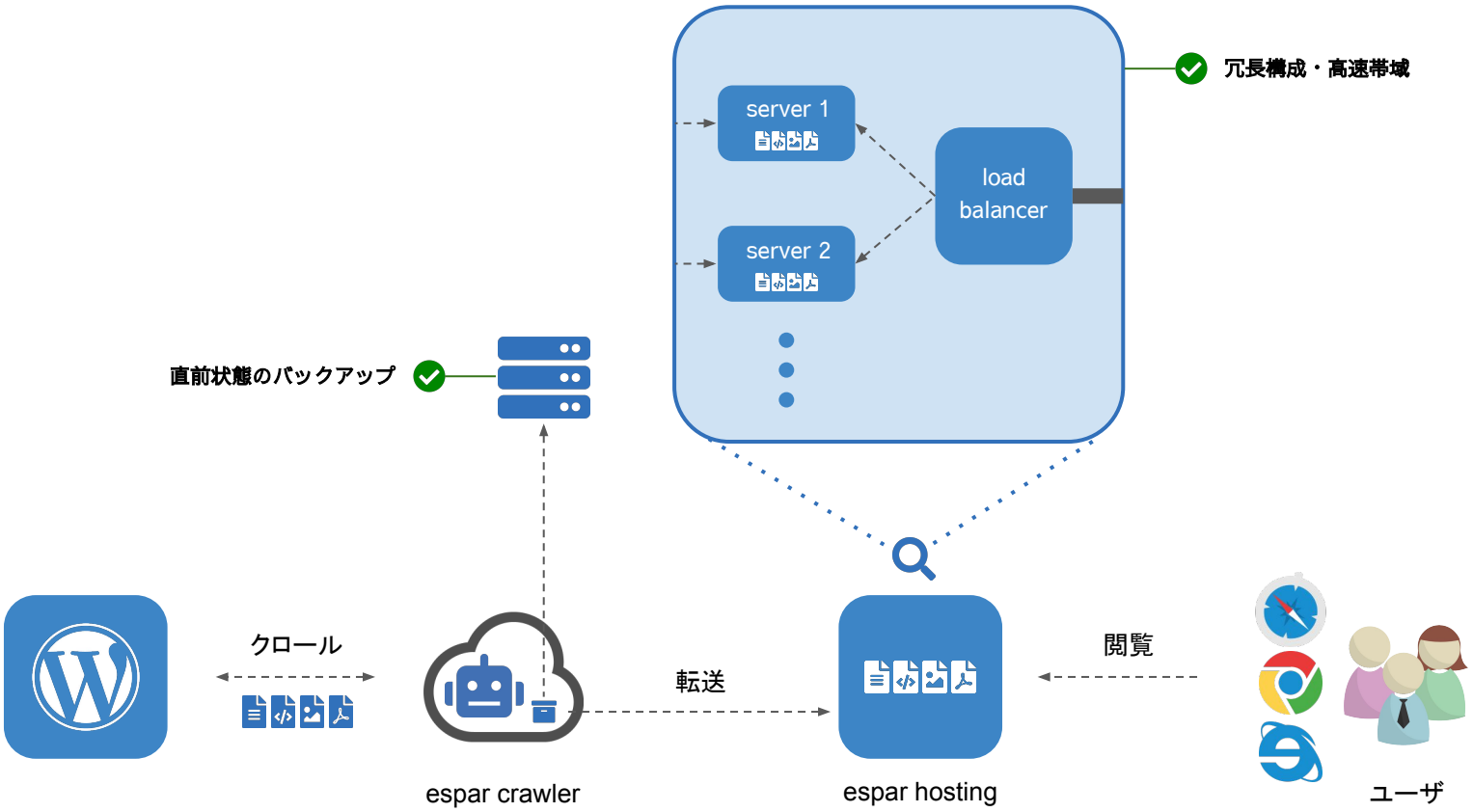
定評ある監視サービスを使用してサイトの公開状態を常に監視しています。負荷の急増や応答不可状態を検出した場合は当社に通知され、早急に回復処理を行う体制を確保しています。

Certification



常時SSL化の為の証明書取得・更新は当社が行います。元WordPressサイトに証明書が設置されていた場合、以後証明書の更新は不要となります。

Backup / Redundancy



espar hosting は単一のサーバではなく、ロードバランサーによる負荷分散機構を備えています。またアクセス急増時に転送速度が落ちないよう十分な上流帯域を確保しています。

また、静的化されたファイル群は物理的に離れた別のストレージにバックアップ保管しています。espar hosting が万が一落ちてしまった場合でも、サイトの公開状態を速やかに復旧できる体制を整えています。