Engineer 技術助言

セキュリティへの取り組み

Engineer ApSの安全な構築・運用の方法をご紹介します。日々の実践、このサイトの保護、脆弱性の報告先を説明しています。

セキュリティは、別売りのサービスではありません。仕事の進め方そのものです。脅威モデルを設計に、防御の強化を構築に、裏付けを引き継ぎに含めます。

最初から制御を設計する

アクセス、デプロイ、復旧を、最初から技術設計の一部にしましょう。

サービスを見る お問い合わせ →

セキュリティの主張の裏付けを見る

セキュリティに関する主張を支える設定やテストを、対象範囲も明確にしたうえでお求めください。

事例 お問い合わせ →

構築の方法

- **標準で最小権限に。** サービスは、それぞれ専用の非特権ユーザーとして、稼働に必要な最小限のアクセスだけで動作します。アクセス境界は、一つのコンポーネントが侵害された場合に、他のコンポーネントへの移動を制限するよう設計しています。
- **シークレットをリポジトリに入れません。** 認証情報はシークレット保管庫またはデプロイ層に置き、ソースにもビルド成果物にも含めません。コミットごとに自動スキャンを行い、検出があればコミットを止めます。
- **インフラをコードで記述します。** 読み、レビューし、再構築できる記述からサーバーを構築します。マシンの設定を、誰かの記憶ではなく、バージョン管理された文書にします。
- **依存関係を固定し、監査します。** システムの構成要素を書き出し、先月動いたからと信じるのではなく、公開されたセキュリティ勧告と照合します。
- **すべての通信を暗号化します。** 証明書の発行と更新を自動化し、更新を監視します。TLSでは、監視されていなかった証明書が障害の原因になりがちだからです。

- **バックアップの自動化と個別の復元テスト。** 誰かが復元するまでは、バックアップは主張にすぎません。バックアップと復元テストのワークフローを別々に実装し、実際に復元して確認したデータに基づいて検証します。

ここまでに挙げたことはすべて **日々の仕事の一部です** — 最後に付け足す工程ではありません。

設計の一部として、セキュリティの範囲、責任、検証方法を合意しましょう。

このサイトの構成

自社サイトにも同じ基準を適用しています。以下の記述は、どれもご自身のブラウザーから確認できます。

- **バックエンドもデータベースも管理者ログインもありません。** 各ページは、要求を受ける前に書き出した静的ファイルです。アプリケーションのセッションやデータベースへのクエリ用エンドポイントを設けないことで、サイトのアプリケーション層の攻撃対象領域を減らしています。
- **実行可能なJavaScriptはゼロ。** ページ、メニュー、リンクにはHTMLとCSSの標準機能を使い、構造化データは実行されないJSON-LDです。リクエストを送ったり設定を保存したりするブラウザースクリプトはありません。
- **厳格なContent Security Policy。** ページ自体に宣言し、`form-action 'none'` を指定しています。サイトはどこにもフォームを送信しません。
- **スタイルシートにSubresource Integrityを適用。** ビルド時にバンドルのフィンガープリントとハッシュを計算し、改変されずに届いたことをブラウザーが検証できます。
- **第三者へのリクエストはありません。** 第三者のアクセス解析、フォント配信サービス、地図ウィジェットはなく、同意バナーもありません。ブラウザーのネットワークパネルを開いてホスト数を数えると、一つだけで、それは私たちのものです。
- **Cookieはありません。** 保存するものとしないものの全容は、Cookieのページに記載しています。
- **機械可読な脆弱性開示方針。** `/.well-known/security.txt` に掲載し、何かを見つけた研究者が、尋ねなくても報告先を確認できるようにしています。

運用の方法

トロントにある小さなサーバー一台を、コードで記述して運用しています。アクセスログは書き込み時にアドレスの一部を伏せ、約三十日間保持します。クレジットにはすべてのソフトウェアを、プライバシーには応答時に記録する情報を正確に記載しています。

脆弱性の報告

このサイト、または私たちが運用するものに弱点を見つけた場合は、発見した内容と再現方法を添えて、welcome@engineer.companyにお送りください。受領を確認し、対応内容をお伝えし、ご希望であれば発見者としてお名前を掲載します。報奨金制度も法的な威嚇もありません。エンジニアに直接届く連絡先があります。

お客様のシステムにも同じ厳密さをご希望でしたら、確認をご依頼ください。

このページの記述は **ご自身で検証できます** — 今お使いのブラウザーから。

バックエンドもCookieもなく、実行可能なJavaScriptはゼロで、ポリシーもページ自体で宣言しています。

自社サイトの確認を依頼する 提供するサービス →

保護が必要なものを明らかにする

保護するシステムの資産、信頼境界、権限を整理するところから始めましょう。

料金を見る お問い合わせ →

対象を絞ったセキュリティ業務を合意する

具体的な制御と受入検査を伴う、範囲を絞ったレビューや実装をご相談ください。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://advisory.engineer.company/ja/security/