Engineer

nonce付きCSPでアプリケーションを堅牢化

nonce付きCSP、HSTS、SameSite Cookie、最小権限のデータベースロール、サーバー側の利用権限再検証により、アプリケーションを堅牢化した。

2025

ブラウザーが敵対的でも機能する防御

状況. 専門家と組織の情報を扱う以上、適切な取り扱いが期待され、防御線1つでは不十分だった。ブラウザー側の制限は操作者が解除できるという、クライアントを敵対的とみなす前提で、それでも安全性を保つ必要があった。

課題. 画面が何を許すかとは独立してサーバーが制御できるよう、フロントエンド、API、DBの各層を堅牢化する必要があった。

行動. Next.jsのproxy.tsで、要求ごとのnonceとstrict-dynamicを持つCSP、HSTS、SameSite Cookieを設定し、ブラウザーの実行と送信を制限した。APIにはレート制限、CORS、サイズ上限、DBへ渡す前の入力検証、セキュリティ関連イベントのログを設けた。DBにはアプリ関数のEXECUTEのみを持つ最小権限ロールで接続し、関数はSECURITY DEFINERとし、すべてパラメーター化した。利用プラン、ロール、組織、船舶範囲の権限を毎回サーバーで再検証し、画面の制限はUXとしてのみ扱った。何が見えるかは画面、何を実行できるかはサーバーが決める。

結果. UIが想定どおり動くことに安全性が依存しなくなった。単一の制御に依存しないよう、防御を多層化した。サーバー側の認可はクライアント側の検証から独立して機能するよう設計し、画面をアクセス判断の根拠にしない構成とした。

この経験をお客様のプロジェクトに

「nonce付きCSPでアプリケーションを堅牢化」を、お客様の組織の似た課題を考える出発点にしてください。この実績を支えたサービスを、お客様のプロジェクトにも提供できます。 データの保存先、処理のルール、他のシステムとの接続方法など、利用者の目に見えない部分をつくります。

サービスを見る お問い合わせ →

結果の背景を確かめる

この事例の状況、判断、結果をご覧ください。どの部分がお客様の制約の下でも生かせるか、どこに別の方法が必要かをご相談いただけます。 nonce付きCSPでアプリケーションを堅牢化 — ブラウザーが敵対的でも機能する防御

サービスを見る お問い合わせ →

アプリケーションは本当に安全ですか？

納品を担当するエンジニアに、プロジェクトについてご相談ください。着手前に、業務範囲、価格の算定方法、引き継ぎ内容を書面で合意します。

担当した役割：セキュリティエンジニア。 関連する分野： プラットフォーム設計, バックエンド開発, フロントエンド開発, API・システム連携, データベース および セキュリティ. こちらのサービスも得意としています バックエンド・API開発 および セキュリティ・アクセス管理.

お問い合わせ サービスを見る

より多くの実績の **一つです** — そのすべてをこのサイトで公開しています。

どの項目も、状況、課題、実施内容、変化という同じ構成で記載しています。

すべての実績を見る

必要な改善を定める

業務の流れ、既存のインターフェース、変更を必要とする利用者をお知らせください。検証可能な納品内容と、お客様のチームが保守を続けられる引き継ぎ内容を定められます。

料金を見る お問い合わせ →

アプリケーションは本当に安全ですか？

「nonce付きCSPでアプリケーションを堅牢化」の判断の背景についてお尋ねください。仕事内容を説明し、お客様のプロジェクトを検討できる担当者が対応します。

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://engineer.company/ja/portfolio/hardened-the-application-with-nonce-based-csp/