インフラエンジニア向け

セキュリティチェックマニュアル

Security Check Manual

Author 馬場 俊彰（ばば としあき）
㈱ハートビーツ CTO
Twitter @netmarkjp

はじめに

セキュリティは情報システムにおいて必要不可欠で不可分な要素ではあるものの、絶対に主役にはならない要素です。そのためセキュリティの作り込みは地味に見えがちですが、インフラエンジニアという「守り支える立場」からすると、絶対に外せないポイントです。数ある非機能要件の中でもとくに、何をどの程度仕込むべきかの**妥当な“セン”の見極め**が難しい項目だと思います。

本稿では一般的なWebシステム（政治的・金銭的な重要度・注目度がとくに高いとは言えないサイト）を前提に、インフラエンジニアの視点でチェックすべきポイントを紹介します。

セキュリティについて検討する場合の鉄則

全体を通しての鉄則があります。とにかく大事なことは、プラクティスに乗ることです。すなわち、

創意工夫しない、オリジナリティを発揮しない、発明しない

ということです。

現在出回っているプラクティスはさまざまな原則や知見・経験に支えられています。それらは世界中の先人たちが苦労して傷つきながら獲得してきたものであり、再発明に挑む必要はありません。創意工夫は楽しいですが、素人の創意工夫は蟻の一穴を仕込むだけなので百害あって一利なし。セキュリティにおいては、そういった一番弱い個所の強度がシステム全体のセキュリティ強度になります。素直にプラクティスに乗りましょう。

まずは「妥当な品質」について合意する

セキュリティはいくらでもコスト・時間をかけられます。コスト（お金や工数）・時間をかければ品質を上げることができますが、現実問題として、品質が高ければ高いほど良いというわけではないので、設計フェーズで妥当な品質をプロジェクトオーナーと合意する必要があります。

品質水準が変わると実施内容は大きく変わります。品質水準が変わり、要求事項が1つ増えただけで利用基盤の変更やシステム再構築が必要になることも十分にあり得るので、ガッチリと合意しておきましょう。

必要な項目を網羅するためのフレームワークとしては、IPAが公開した非機能要求グレード[注1]がお勧めです。

……と書いてはみたものの、非機能要求グレードをもとにした整理に付き合ってくれるプロジェクトオーナーはそうそういません。そこでお勧めしているのが、実際にニュースになった事例を使ったケーススタディです。実名を出すのは控えますが、

注1）「非機能要求の見える化と確認の手段を実現する「非機能要求グレード」の公開：IPA独立行政法人情報処理推進機構」
URL https://www.ipa.go.jp/sec/softwareengineering/reports/20100416.html