

平成25年度秋期 応用情報技術者試験 午後問8 (Webサイトセキュリティ) 徹底復習レポート

1. 導入：Webサイト更改におけるセキュリティ設計の戦略的重要性

A社が実施したWebサイト更改は、単なるビジュアルの刷新ではなく、ビジネスモデルを「静的な情報提供」から「動的なパーソナライズド・サービス」へと進化させる戦略的な転換です。ユーザサポート向上のために導入された会員専用サイトでは、ユーザIDとパスワードによる認証が行われ、購入履歴等に基づいた技術情報が動的に生成されます。この移行において、守るべき資産は「一般公開情報」から、極めて機密性の高い「個人の認証情報」や「個別提供の技術情報」へと変化しました。動的なWebアプリケーションは利便性が高い反面、攻撃対象領域（アタックサーフェス）を拡大させます。ここでのセキュリティ設計の不備は、顧客情報の流出やサイト改ざんによる信頼失墜を招き、ビジネス継続性に致命的な打撃を与えかねません。そのため、開発（セキュアプログラミング）とインフラ（多層防御）の両面から強固な防御策を講じることが、更改プロジェクトにおける最優先の成功要因となります。

2. 懸念される4つの脅威とビジネスインパクトの評価

A社のセキュリティ担当課長が挙げた4つの脅威は、現代のWebビジネスが直面する主要なリスクを射抜いています。

- **認証情報の盗聴：** インターネット上の通信が平文の場合、悪意のある第三者に **ユーザID** や **パスワード** を盗み見られるリスクです。これにより、会員へのなりすまし被害が発生します。
- **Webサイトの改ざん：** Webサーバが外部から直接攻撃可能な状態にあると、コンテンツが書き換えられ、企業の社会的信用の失墜や、閲覧者をウイルス感染サイトへ誘導する踏み台にされる恐れがあります。
- **SQLインジェクション：** 入力フォーム等から不正なSQL文を「注入」し、DBを操作する攻撃です。会員情報の組織的な漏洩やデータの破壊を招く、極めて深刻な脅威です。
- **クロスサイトスクリプティング (XSS)：** ユーザのブラウザ上で不正なスクリプトを実行させる攻撃です。Cookieの奪取によるセッションハイジャックや、偽画面への誘導が行われます。**【指導者視点：対策の相互関連性】** これらの脅威は独立しているわけではありません。例えば、XSSで奪ったCookieや盗聴した認証情報を用いて正規ユーザになりすまし、その後に内部からSQLインジェクションを試行するといった複合攻撃が典型的です。したがって、対策も「点」ではなく「面」で捉える必要があります。

3. セキュリティ強化策の三段構え：多層防御の構造分析

A社は「多層防御」の原則に基づき、以下の3つの対策を垂直に積み重ねることで、一箇所の防御が破られても全体が崩壊しない構造を構築しました。

(1) データ暗号化 (HTTPS) による秘匿性の確保

下線①が示す「暗号化すべきデータ」の正体は、認証に直結する **ユーザID** および **パスワード** です。HTTPアクセスをHTTPSへ強制リダイレクトする仕組みを導入することで、ユーザの過失による平文通信を排除し、「認証情報の盗聴」を確実に阻止します。

(2) ネットワーク隔離とリバースプロキシによる要塞化

WebサーバをDMZから内部LANへと移設し、インターネットからの直接アクセスを遮断しました。外部との通信はリバースプロキシサーバが代理 (プロキシ) することで、WebサーバのIPアドレスや構成を隠蔽します。これは「Webサイトの改ざん」に対する強力な抑止力となります。

(3) WAF (Web Application Firewall) による高度な検査

リバースプロキシサーバに実装されたWAFは、**ブラックリスト方式** (既知の攻撃パターンとの照合) を用いてリクエストを精査します。 **【戦略的ポイント】** WAFとセキュアプログラミングは「二重のチェック機能」として働きます。開発時のコード修正で見落としした脆弱性をWAFがインフラ層で防ぎ、逆にWAFをすり抜ける未知の攻撃をアプリケーション側のサニタイジングが防ぎます。これにより、SQLインジェクションやXSSといったアプリ層の攻撃を効果的に遮断します。

4. SSLサーバ証明書の取得と実装プロセスの精査

HTTPS通信を「信頼できるもの」にするためには、公開鍵基盤 (PKI) に基づいたSSLサーバ証明書の実装が不可欠です。

1. **証明書の実装フロー:**
2. **CSR (証明書署名要求) の生成:** サイトの身元を示す「識別名 (DN)」と**c 公開鍵**を含んだCSRを作成します。コモンネーム (FQDN) には、サービスURLのドメイン部分である `www.a.co.jp` を正確に設定する必要があります。
3. **証明書の発行と導入:** 認証局から発行された**a SSLサーバ証明書 を機器に導入する際は、ペアとなる d 秘密鍵**が必須です。このペアが揃って初めて、サーバの正当性が証明され、暗号化通信が可能になります。
4. **ロードバランサへの導入とその必然性:** 本事例において、SSLサーバ証明書は **ロードバランサ** に導入されています。 **【試験対策上の重要ポイント】** ロードバランサは「Cookieの情報」に基づいてセッション維持 (振り分け) を行います。通信が暗号化されたままでは、ロードバランサはCookieの内容を読み取ることができません。したがって、**「Cookieの情報を参照するために、HTTPS通信を復号して平文にする必要がある」** (SSL終端) という技術的必然性から、この導入ポイントが選定されています。

5. 運用フェーズにおけるインシデント分析: セキュリティ警告の正体

運用開始から1年後、ユーザに表示された「セキュリティの警告」は、システムライフサイクル管理の重要性を突きつける事象です。図2のメッセージにある「有効期間に問題があります」という記述から、原因が **SSLサーバ証明書の有効期限切れ** であることは明白です。

【講師のアドバイス: 原因の特定】 試験問題において「運用開始から1年後」という具体

的な期間が示された場合、多くのケースで証明書の標準的な有効期限（1年単位）を暗示しています。クライアントPCの時計の狂いも可能性としてはありますが、ビジネス環境においてはサーバ側の期限管理漏れを第一に疑うのが定石です。このインシデントに対し、管理者が取るべき適切な対応は**「SSLサーバ証明書の更新（再取得）申請を行う」**ことです。証明書は「信頼のチェーン」によって成立しているため、一時的な無視やクライアント側の設定変更ではなく、認証局を通じた正規の手続きによる根本解決がビジネス継続性の観点から唯一の正解となります。

6. 結論：本事例から学ぶWebセキュリティのベストプラクティス

本事例は、応用情報技術者試験の頻出テーマである「Webアプリケーション」と「ネットワークインフラ」の統合的な視点を提供しています。

1. **設計段階の多層防御：** HTTPSによる盗聴防止、WAFによるアプリ保護、ネットワーク隔離によるサーバ保護の3軸を揃えること。
2. **インフラの整合性：** ロードバランサでのSSL終端のように、アプリケーションの要件（Cookie参照）とインフラの制約を整合させる設計能力。
3. **ライフサイクルの維持：** 堅牢なシステムを構築しても、証明書の更新管理といった基本的な運用が欠ければ、サービスは容易に停止（または警告表示）に追い込まれるという教訓。セキュリティの専門家には、個々の技術要素を理解するだけでなく、それらがビジネス資産をどう守り、運用の中でどう維持されるかという「大局的な視点」が求められます。本レポートの内容を、実務におけるセキュアなシステム運営の指針として活用してください。