別紙

「ウェブ健康診断仕様」の内容：

「ウェブ健康診断仕様」には診断項目ごとに、検出パターンと、それに対応した脆弱性有無の判定基準が記載されています。診断を行う際には、検出パターンに従った入力を診断対象サイトに対して行い、その出力や動作を解釈して、脆弱性有無を判定します。もし脆弱性があった場合、「安全なウェブサイトの作り方」本編を参考に解決策の検討が行えます。

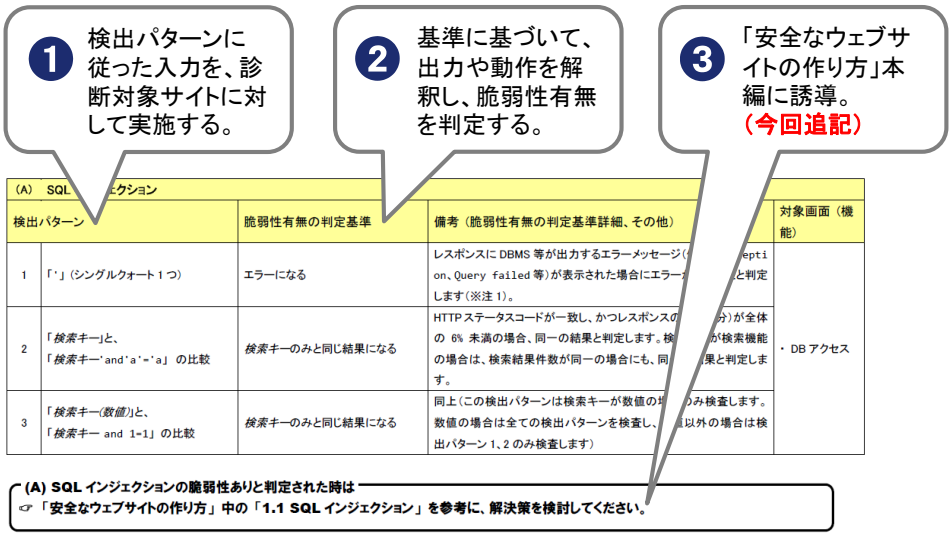

図:「ウェブ健康診断仕様」内容と使い方

「ウェブ健康診断仕様」の診断項目：

「ウェブ健康診断仕様」には、危険度の高い脆弱性や、Web アプリケーション脆弱性診断事業（LASDEC 実施）で検出数の多かったものなど、13 の診断項目があります。

(A) SQL インジェクション
(B) クロスサイト・スクリプティング
(C) CSRF（クロスサイト・リクエスト・フォージェリ）
(D) OS コマンド・インジェクション
(E) ディレクトリ・リスティング
(F) メールヘッダ・インジェクション
(G) パス名パラメータの未チェック／ディレクトリ・トラバーサル
(H) 意図しないリダイレクト
(I) HTTP ヘッダ・インジェクション
(J) 認証
(K) セッション管理の不備
(L) 認可制御の不備、欠落
(M) クローラへの耐性

「ウェブ健康診断仕様」の使用上の注意：

「ウェブ健康診断仕様」の診断は、**検査パターンを絞り込んだ診断**ですので、脆弱性が検出されなかった場合でも、**安全宣言には繋がりません**。診断の結果を確認した後は、より詳細な診断を受けたり、「安全なウェブサイトの作り方」を参考に対策を実装することなどを推奨します。