



## 【「IBPS Web アプリケーション検査サービス」料金体系】

|                                        |                      |
|----------------------------------------|----------------------|
| Web アプリケーションへのセキュリティ検査 <sup>(*)2</sup> | ページ単価：82,000 円～      |
| 検査後の脆弱性に対しての再検査(オプション) <sup>(*)3</sup> | 200,000 円(インターネット経由) |

<sup>(\*)2</sup> ページ単価は総検査ページ枚数によって変動いたします。

<sup>(\*)2</sup> オンサイトでの検査の場合は、別途出張費が必要になる場合がございます。

<sup>(\*)3</sup> 再検査実施は、簡易速報提示後 1 ヶ月以内に行うことを条件とします。

<sup>(\*)3</sup> 再検査の対象は、ページ数や脆弱性には依存しません。但し、再検査実施に 1 日以上を要する場合には、別途料金をいただく場合がございます。

## 【レポートサンプル】

4.2 危険度【**高**】の指摘事項

4.2.1 **SQL インジェクションの脆弱性**

【危険度】**高** 【攻撃難易度】**低**

【説明】

予約詳細内容確認画面(showreservation.php)では、ユーザからの入力チェックがされていないため SQL 文に渡されているため、以下のような入力を行うことで、全登録会員の予約状況を閲覧することが可能です。(図表 2 参照)

・ `http://secure-aiways/showreservation.php?rsid="" or RSID like "%&sid=a20103060825`

このため、全登録会員の個人情報(氏名、住所、電話番号)や予約情報が漏洩してしまいます。

【推奨】

ユーザから入力される全てのデータは入力チェックを毎回実施してください。ユーザからの入力を SQL 文に渡す場合は、適切なサニタイジング(悪意ある)処理を実施し、SQL 文として解釈させないようにしてください。

図表 2：SQL インジェクションの脆弱性

The screenshot shows a web browser window displaying a reservation list. Two red boxes highlight the input fields for 'お客氏先名称' (Customer Name) and 'お客氏先住所' (Customer Address). A blue box with the text 'SQL 構文を入力' (Enter SQL syntax) points to the input field for 'お客氏先住所'. The reservation list includes details such as reservation ID, date, time, and location.

## 報道関係問合せ先

IIJ グループ広報室 池田、手島

TEL: 03-5259-6310 FAX: 03-5259-6311

E-mail: [press@ij.ad.jp](mailto:press@ij.ad.jp) URL: <http://www.ij.ad.jp/>

## 営業関係問合せ先

株式会社アイアイジェイテクノロジー 営業企画室

TEL: 03-5205-6703 E-mail: [info@ij-tech.co.jp](mailto:info@ij-tech.co.jp)