

Webアプリ診断サービス - 今、Webアプリが狙われています -

攻撃対象が変化しています！

◆ 攻撃対象の変遷

- 従来：OSの脆弱性を突いた攻撃
 現在：Webアプリの脆弱性を突いた攻撃
- ・SQLインジェクション
 - ・クロスサイトスクリプティング

例. 某音響機器販売社

- 外部からの不正侵入による**9万7千人分**の
 個人情報情報が漏洩
 <影響>
- ・約1ヶ月超のクレジット通販業務の停止
 - ・高額な調査費用、顧客への賠償費用
 - ・顧客の信頼度低下

解決案

・Webアプリに存在する脆弱性を把握したい

- 最新の情報によるツールを用いた診断
 ・脆弱性や脅威のレベルによる対策優先順位付け

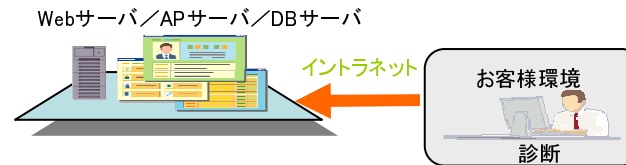
効果として・・・

- ・残存リスクが明確になる
- ・実施すべき対処が明確になる

Webアプリ診断サービス

Webアプリに潜む脅威を発見

発見された脅威には、優先順位と対策方法を提示



■ 診断内容

⇒ファイアウォールや侵入検知システムでは防御、検知できないWebアプリの脅威 (SQLインジェクションやクロスサイトスクリプティングなど) に対する安全性を診断します。

■ 報告内容

⇒膨大な診断結果からエキスパートが脅威を分析
 ⇒脅威をランク付けし、対処の優先順位を支援
 ⇒具体的な対処方法を掲載

Webアプリの脆弱性を突いた攻撃を防ぐために

なぜWebアプリの脆弱性を突いた攻撃を受けるのか？

運用しているWebアプリに脆弱性があり、その脆弱性に対して対策がとられていない可能性があるため

どうすれば防止できるのか？

脆弱性のないWebアプリを運用する

そのためにはまず何をすべきか？

Webアプリに脆弱性があるかないか
リスクを可視化することが重要

【お問い合わせ先】 株式会社 富士通九州システムズ (FJQS)

東京オフィス 〒144-0035 東京都大田区南蒲田2-16-2 テクノポート三井生命ビル9F

Tel. 03-5703-7028 Fax. 03-5703-7050 (担当:セキュリティセンター)

大分事業所 〒870-8551 大分県大分市東春日町17-58 (ソフトパーク内)

Tel. 097-534-8119 Fax. 097-535-1064

2009. 10