

サーバを脅かす脆弱性

- ◆パッチ未適用によるワーム感染
未適用パッチの脆弱性を悪用され、サーバが感染し、別サーバやクライアントまで被害が及んだ
- ◆USBメディアなどからウイルス感染
ウイルス感染しているUSBメモリやCD-ROMを挿入しただけで感染した
- ◆重要なシステムファイルの改ざん
システムファイルの不適切なアクセス権を悪用され情報改ざんやサービス停止など業務妨害を受けた
- ◆離職者アカウントの悪用
離職者のアカウントを放置していたため、悪用されて情報が漏えい

必要な対策と課題

重要なパッチの適用が必要

重要なファイルに適切なアクセス権設定が必要

OSやアプリケーションのバージョンアップが必要

課題

適用すべきパッチの切り分けが大変

不適切なアクセス権や設定を見過ごしていた

古いOSやアプリの使用によるリスクが分からない

解決案

- ・サーバに存在する脆弱性を確認したい
- ・効果的な対処を実施したい

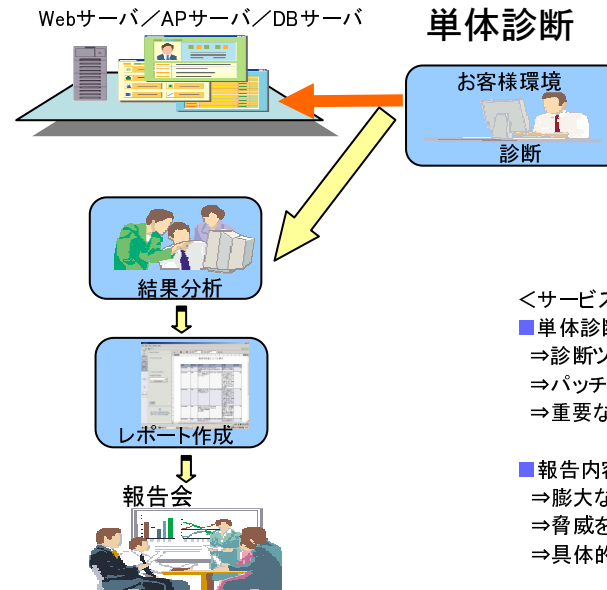
- ・最新の脆弱性情報によるツールを用いた診断
- ・危険度ベースの対策優先順位付け

- 効果として・・・
- ・脆弱性を発見
 - ・優先順位付けによる効果的な対処の実施

サーバセキュリティ診断サービス

サーバ自身に潜む脅威を発見

発見された脅威には、優先順位と対策方法を提示



<サービス内容>

- 単体診断
 - ⇒診断ツールをサーバにインストールし、診断
 - ⇒パッチ適用状況を診断
 - ⇒重要なシステムファイルの設定やアクセス権を診断
- 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

【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. 6