

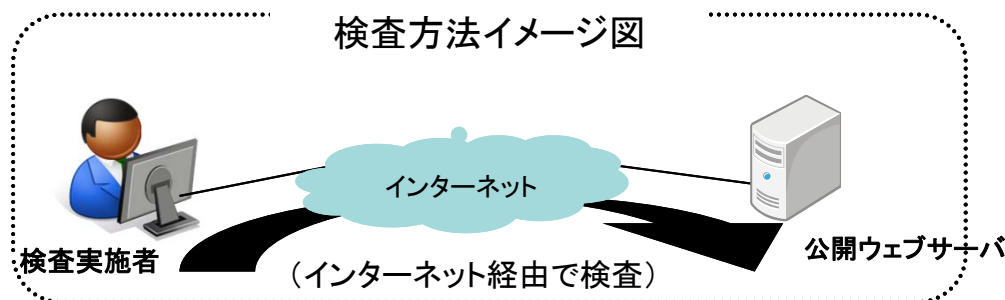
脆弱性検査状況報告(概要)

1. 検査期間:平成23年9月～12月
2. 検査対象:政府機関における公開ウェブサーバ(検査希望のあった11省庁、約330画面)
3. 検査方法:対象とする公開ウェブサーバにインターネット経由でアクセスし、ツール及び手動により検査を実施
4. 検査内容:プラットフォームに関する検査
ウェブアプリケーションに関する検査
5. 検査結果:検出された脆弱性のうち緊急性の高いものについては、当該府省庁に対し速報を発出し、対策を実施済み又は実施中
検査結果については、今後、全府省庁に対して情報共有を行い、政府機関全体の情報セキュリティ対策の向上に活用する予定

検査工程

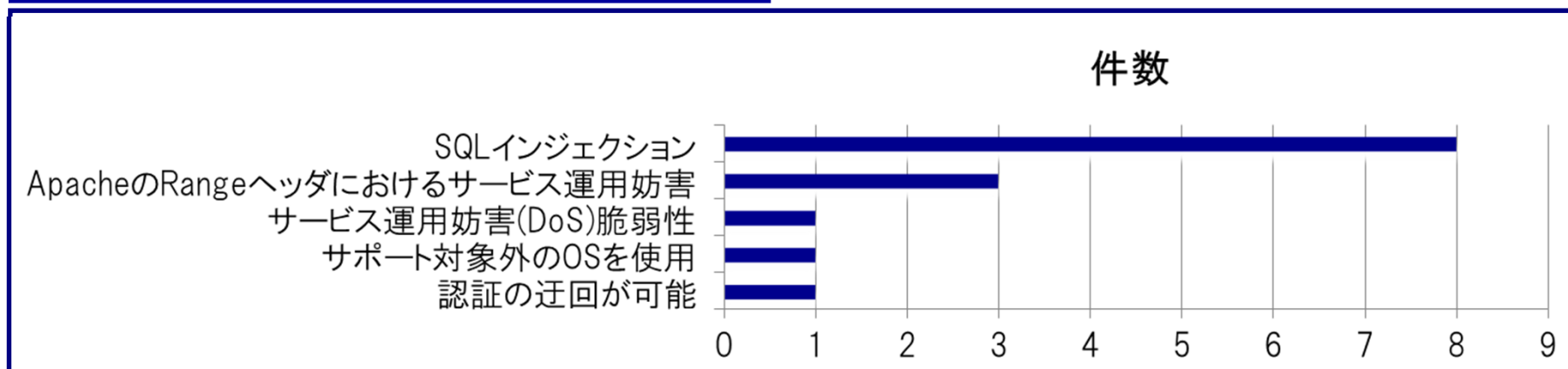
	7月	8月	9月	10月	11月	12月	1月
希望調査	▶						
検査実施			▶				
結果報告						▶	

検査方法イメージ図



「脆弱性検査」結果

危険度「高」の検出結果(延べ14件)



	脆弱性内容	原因	想定される被害
1	SQLインジェクション	ウェブアプリケーションにおいて、入力値チェックやエスケープ処理が徹底されていない	データベースに格納されている情報の漏えい、改ざん、破壊等の可能性
2	ApacheのRangeヘッダにおけるサービス運用妨害	パッチ未適用	サービス運用妨害(DoS)により、サーバが停止する可能性
3	サービス運用妨害	ハードスペックやソフトウェア設定において、システム導入時に見積もった内容が実運用時のデータ送信量に対し過少である可能性	サービス運用妨害(DoS)により、サーバが停止する可能性
4	サポート対象外のOSを使用	—	パッチ適用による対策が行えず、セキュリティ侵害が発生する可能性
5	認証の迂回が可能	ウェブアプリケーションにおいて、ログイン処理の成功、不成功にかかわらずアクセス可能なプログラムになっていた可能性	IDとパスワードを入力せずにログイン後のページにアクセスでき、情報漏えい等の可能性