JNSA ワーキンググループ紹介

Webセキュリティ調査・検証WG

Ｗｅｂセキュリティ調査・検証WGリーダー
株式会社アークン
斉藤　純平

■はじめに

ここ数年、企業のビジネスを左右する情報や機密性の高いデータなどが、Internet上に公開されたWebサーバおよびデータベースサーバに格納されています。しかし、「サイバーテロやインターネットセキュリティ侵犯の75%は、インターネットアプリケーションによって発生する」(2002年：Gartnerレポート)といわれるように、現在Webが、重要なIT資産の情報漏えい、改ざん、不正利用といった脅威にさらされています。また、攻撃手法もこれらの状況の変化により変わってきています。以下一例を示しますが、これらの攻撃はブラウザ経由で行われるためファイアウォールでは防ぐことが出来ない特徴があります。

- **SQLインジェクション攻撃**
  Webの作り方によっては、ブラウザ経由でバックグラウンドで動作するDataBaseからDataを抜き出すことが出来る。
- **クッキー改ざん攻撃**
  ECサイトで商品購入情報を保存しているクッキーを改ざんすることにより割引価格で購入可能。
- **パラメータ改ざん攻撃**
  会員専用サイトなどで簡単なセッションIDを使用していると一旦正会員としてサインイン後URLのセッションIDを変更することにより他の会員になりすまし、他の会員の情報を閲覧可能。

■活動目的

本年度より活動を開始するWebセキュリティ調査・検証WGでは、組織にとって近年益々重要な基盤となっているWeb環境に特化した攻撃手法やその対策を調査・研究します。

本年度の活動はWebの脆弱性・Webに特化した攻撃手法の調査、および具体的な対策の調査を行います。また、攻撃検知・防御ソリューションによる対策については検証環境を構築した上で検証を行います。

■今後の予定

現在、Web開発の立場、Webの脆弱性を診断する立場、Web診断ツール・Webアプリケーションファイアウォールベンダーの立場の方々を中心に33名がWGに参加いただいております。

本年度は、診断チーム、開発チーム、WAFW(Web Application Firewall)チームの3つに分かれ以下の成果物を目標に活動を行うこととなりました。

- **診断チーム**　「Webセキュリティ診断ガイドライン」
- **開発チーム**　「セキュアWebアプリ開発ガイドライン」
- **WAFWチーム**「Web Application Firewall製品選定のガイドライン」
- **全体**　「脆弱性分類表」、「WG活動報告書」

また、実際の検証に際してはどこまで本年度中に出来るか解りませんが以下を予定しています。

- 脆弱版Webアプリケーション VS 診断チーム
- セキュア版WebアプリVS診断チーム
- Web Application Firewall(デフォルト)VS診断チーム
- Web Application Firewall(チューニング済)VS診断チーム

今後ますます重要になってくるWebアプリケーションセキュリティに関し、JNSAならではの成果物を出すべく活動を行っていければと考えています。