Webアプリケーションセキュリティ WG

WGリーダー
住商情報システム株式会社　二木　真明

■ はじめに

昨今、またWebサイトが攻撃を受け、改ざんや情報漏洩が発生するという事件が頻発しています。セキュリティ対策はすでに万全と思われていたサイトがなぜ、このような事態に陥ったのでしょう。原因は、Webサーバやそのオペレーティングシステムの脆弱性ではなく、ユーザ自身が開発し、運用していたWebアプリケーションにありました。不正な入力を与えることで、アプリケーションが誤動作し、開発者が意図しない動作をしてしまったのです。大規模な顧客、会員データベースなどと直結して動作することも多いこれらのアプリケーションが誤動作することによる影響は、インフラの脆弱性以上に危険なものです。この点が、これまでのセキュリティ対策の盲点でした。

WebアプリケーションセキュリティWGでは、こうしたアプリケーションの脆弱性対策に焦点をあて、様々な研究活動、啓発活動を展開していきます。

■ 主な活動内容

Webアプリケーションセキュリティを考える場合、ソフトウエア開発、脆弱性検査、監査、侵入検知と防御など、様々な切り口があります。また、こうした切り口からのアプローチには、それぞれの分野での、知識や経験が必要です。今年度のWGでは、こうしたいくつかのアプローチについて分科会形式で検討し、それを全体会でレビューする、という形をとります。現在、作業が進んでいる分科会としては、以下のものがあります。

■ 啓発コンテンツ分科会

Webアプリケーションのセキュリティについての一般の認識はまだまだ浅い、と考えられます。これらを少しでも解消するための啓発活動に利用可能なコンテンツ（セミナー用プレゼンテーション）を作ろうというのが、この分科会の目的です。どちらかといえば、マネジメント層向けの「総合」コンテンツ、開発者向けの解説、運用現場向けの解説など、いくつかの切り口からコンテンツを作っていく予定です。また、出来たコンテンツは公開すると同時に、JNSAが企画、参加するイベントなどでのセミナー等にも活用していく予定です。

■ 受発注ガイドライン分科会

Webアプリケーションの問題を解消するには、まず開発の際にきちんとセキュリティを考慮することが必要です。しかし、このための公的なガイドラインは少なく、ともすれば、開発の際に発注側と受注側の認識のずれが生じることになり、後々、責任の所在

などを含めて混乱することも多いようです。この分科会では、ソフトウエアの受発注における、セキュリティの定義方法について検討し、その問題点や解決策などを議論します。可能であれば、発注側、受注側双方がコンセンサスを取りやすい方法をいくつか提示できればと考えています。

■ 技術研究分科会

Webアプリケーションの攻撃手法や脆弱性の検査、防御手法、ツールなどに関する技術的な研究を目的とした分科会です。日頃、こうした業務に携わる技術者が情報や意見を交換しながら、タイムリーなテーマについて研究を行います。また、この分科会は、各分科会からの要請に応じて、技術的な情報や意見を提供する役割も担います。

■ 最後に

Webアプリケーションセキュリティは、様々な側面からの検討が必要です。そういう意味では、もっと多くの分科会があってもいいかもしれません。実際に、こうした業務に携わっている方々、興味を持たれている方々の参加をお待ちしています。