NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

# Webアプリケーションセキュリティ WG

リーダー：二木真明
住商エレクトロニクス（株）

2005年6月13日

## WGの内容

- Webアプリケーションセキュリティに関する調査、研究
  - Webアプリケーションが包含する脆弱性についての検討
  - 脆弱性への対策、回避策の検討
    - アプリケーション開発上での対策
    - 脆弱性の検証方法
    - 運用中のシステムが持つ脆弱性の回避方法
  - Webアプリケーションセキュリティに関する啓蒙活動

# Webアプリケーションセキュリティ

- ＯＳや市販ソフトウエアの脆弱性への対処
  - とにかくパッチをあてる。（最新版を使う）
- 自社開発アプリ、特にWebアプリに存在する脆弱性
  - 入力チェックが不充分であったりすることが原因で、誤動作し、意図しない動き（不要なデータを表示したり・・・）をする
  - たとえば




# 昨年度の活動

- 開発系、検査系、防御系の3チームにて活動
  - 開発系：Webアプリ脆弱性の研究。検証サイトの開発
  - 検査系：Webアプリ脆弱性検査ツールの調査、利用法の検討
  - 防御系：Webアプリケーションファイアウォール製品の調査、利用法の検討
- 残念ながら、メンバー多忙のため夏以降、活動が停滞。成果が出せなかった。
- 本年3月に仕切直し。リーダー多忙のため交代し、再度、ＷＧの目的を含め議論を行った。

# 昨年の反省

- 遠大な計画
  - 検証用サイトの開発・・・・（実際に開発するとなるとかなりのリソースが必要。WGというレベルでは短期には困難）
- サブテーマ間の調整難
  - 検査系、防御系の作業が「検証サイト」完成を前提としていた点
- メンバーの業務状況を甘く見ていた点
  - 年度後半、リーダー、メンバーともに多忙な状況で活動が停止。
  - 前半勝負で作業する必要性




# 今年度の方向性

- まとまった成果物を一気に目指すのではなく、比較的軽い（2ヶ月から3ヶ月で完成できるような）テーマを複数設定して、順次完成させていく
- ターゲットを明確にする。
  - 誰のための成果物か
  - 何のために、どのようなものを提供するのか

# 今年度の分科会テーマ

- Webアプリケーションセキュリティに関する啓蒙コンテンツの作成
  - まだまだ啓蒙フェーズにあるWebアプリケーションセキュリティをわかりやすく解説。テーマごとに小さなプレゼンを複数準備する。
  - 最終的には1日セミナーが可能な程度のコンテンツ作成と、可能ならばセミナー実施を目指す。
- Webアプリケーション開発の受発注におけるセキュリティガイドラインの検討
  - 発注側、受注側のコンセンサスがとれ、検収条件としても利用が可能なものがない現状があり、これを作りたい
  - 政策部会：セキュア開発ガイドラインWGとのコラボ
- 攻撃手法の技術的研究
  - 攻撃手法を詳細に研究し、様々なパターンや危険性を明らかにする。（クロスサイトスクリプティングだけをとっても、非常に奥が深い）




# 作業方法

- 下記テーマごとに小グループに分かれて、独立して作業する
  - 運営は分科会リーダーに一任
- 毎月1回全体会合を持ち、各分科会の作業状況、内容を全員でレビューする
  - これにより、WG全体として成果を共有する