≪ 巻末の付録USBメモリに詳細版を収録 ≫

第14部

ウェブアプリケーションのセキュリティ技術の研究（概要版）

宮本 大輔、Gregory Blanc、門林 雄基

SWAN（Security for Web 2.0 Application）WGでは，最近の悪意あるウェブサイトの動向を観測し対策を検討している．

ウェブを介した攻撃にはその攻撃空間が広いという特徴があり，本研究グループはその広い特性に対応した研究を行なっている．これまでの活動としては，脆弱性を持つウェブ2.0のアプリケーションをWIDEメンバーに提供する試みや，悪意あるウェブサイトによく見られる難読化されたJavaScriptの構造に着目した解析，PCだけではなくAndroidなどで動くマルウェアの解析技術のハンズオンなどが挙げられる．

今年度は，ウェブを悪用した攻撃であるフィッシングサイトに着目した研究を行った．マルウェアではなく人間を騙すことによって攻撃が発生する点でこれまでの研究とは異なるが，SWAN WGでは人間の行動だけではなく，フィッシングサイトをホスティングしているサーバ，関連して発生するネットワークインフラへの影響など，WGの趣旨通り，広い特性を考慮した研究開発を行なっている．

概要は以下に示す．
詳細はwide-memo-SWAN-report2012-00を参照して頂きたい．

- フィッシングサイト検知技術の個人に合わせた調整手法の研究
  フィッシングサイト検知技術はエンドユーザを守るものであるが，その各個人の知識や意思決定基準に応じて対策技術を調節可能とする手法を開発している．アンケートを元に意思決定プロセスを解析し，ユーザタイプに応じたフィッシングサイト対策の方式提案を行った．

- フィッシングサイトの模倣インターネット上での再現
  消滅するのが早いフィッシングサイトを保存し，テストベッド上に再現する研究を行った．また，フィッシングサイト対策技術と他のサイバー攻撃の対策技術が互いに協調したサイバー防御を想定し，このような防御技術を評価するためのテストベッドの研究開発を行った．また，研究の一部について，５月研究会にてポスター展示を行った．

SWAN WGでは引き続き，フィッシングサイトを含む悪意あるウェブサイト全般について，多面的な研究を行なっていく．研究成果は引き続きWIDE研究会及び学会発表を通じて行い，ソフトウェアなどの成果物は必要に応じた公開を検討している．