≪ 巻末の付録USBメモリに詳細版を収録 ≫

第６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，悪意あるウェブサイトの動向を観測し検討している．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，エンドユーザの能力を機械学習と組み合わせ活用するフィッシングサイト解析や，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，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，前年度の成果を発展するべく，エンドユーザの行動を解析する研究をサーベイし，事前実験を開始した．また，採取しているフィッシングサイトについて，いわゆるビッグデータ解析環境にデータを展開することにより他のサイバー脅威との相互な解析を目指す活動を行った．このように，今年度も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．詳細は巻末のUSBメモリに収録された詳細版報告書を参照していただきたい．

・エンドユーザのウェブサイト真贋判定における意思決定パターンの認知心理学に基づいた解析

昨年度実施した，「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」[64] は，フィッシングサイトの判定を各個人に調整するアルゴリズムを調査するべく，エンドユーザの意思決定基準を被験者実験により調べるものであった．本年度は，エンドユーザの生体情報から意思決定を推測しうる情報についてサーベイを行い，結果を論文[65] として発表した．さらに，この知見に基いて視線追跡の活用を試みた．これについて，事前実験の結果を報告する．

・フィッシングサイトのデータベース

昨年度は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．この際に収集したフィッシングサイトのURL や，フィッシングサイトが発見された当時のIP アドレスをデータベースに保存しており，これらの情報をビッグデータ解析環境への移行を行った．この作業内容について報告する．

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．