≪「**報告書詳細版**」は巻末の付録USBメモリに収録しています≫

第９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、藤原 寛高、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，エンドユーザの認知能力に合わせた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，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，多くのWIDEプロジェクトメンバーが参加している日欧協調によるマルチレイヤ脅威分析およびサイバー防御の研究開発（NECOMA）とSWANWGは連携した研究を行い，「アドレスバーを目視で確認する」ことをエンドユーザに習慣として身につけさせる取り組み，2014年WIDE秋合宿で行った被験者実験，そして難読化の特徴を利用したドライブバイダウンロード攻撃検知手法の研究開発を実施した．

概要は以下に示す．詳細はwide-memo-SWAN-report2014-00を参照して頂きたい．

・アドレスバーを目視で確認する習慣
　URLやSSLの鍵アイコンを確認するような習慣をエンドユーザに身につけさせる手法について研究開発を行った．なお，詳細な内容は文献[11]を参照されたい．

・フィッシングサイト判別実験
　2014年WIDE秋合宿参加者を被験者とし，フィッシングサイトと正規サイトの判別実験を行った．被験者は20ウェブサイトのスクリーンショットを閲覧し，フィッシングサイトか否かを判定する．その際に用いた意思決定基準をアンケートによって，また，何を見ていたかを視線追跡カメラによって取得した．

・難読化の特徴を利用したドライブバイダウンロード攻撃検知手法の提案
　難読化は様々な分野で利用されているが，悪性ウェブサイトが解析を困難にするため難読化手法を用いる事例も存在する．本研究では，良性及び悪性の難読化について，複数のデータセットを用いた調査を行った．なお，詳細な内容は文献[12]を参照されたい．

SWAN WGでは引き続き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．