≪「**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８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、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，認知心理学に着目したサイバー防御システムの開発と評価を行った．この研究領域には様々なチャレンジがあるが，その１つに「人間の観測される情報から，人間の精神状態を推測する」という課題がある．例えば人間の精神的負荷の高まりを眼球運動や脳波，血圧，呼吸，顔表面温度などから分析する研究が行われている．ストレスの増加など精神的負荷の高まりは過失を引き起こしやすいとされており，このような課題は人的要因の解決を行っているとも考えられる．さらに，近年のIoT技術の普及に伴い，人間から健康に関するデータを取得する様々な生体センサーの技術開発が進んでいる．この情報を認知心理学の観点から活用すれば，情報機器を利用するユーザが今まさに何を考えているのか，どのような情報を入手し，どのような根拠で，どのような意思決定をしようとしているのかを推測できると思われる．

これまでのサイバーセキュリティ対策では，エンドユーザがどのような状態あるかは考えていないが，仮に「まさに騙されそうな状態にあるユーザ」がわかるのであればどうか．普段は，正常なプログラムをマルウェアであると，正規サイトをフィッシングサイトであるといった誤検知を減らすべく工夫されているセキュリティ技術や製品も，この時ばかりは誤検知を承知の上で注意喚起ができるのではないか．このような工夫によって，人的要因によって起こるインシデントは減らせるのではないか．

SWAN WGではこの観点から研究活動を行った．概要は以下に示す．詳細はwide-memo-SWAN.report2016-00を参照して頂きたい．

・フィッシングサイトと視線の相関分析

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．本報告書では，この分析結果について報告する．

・視線に基づいたサイバー防御を行うシステムの研究開発

フィッシングサイトと視線の相関分析結果で得られた知見を基に，アドレスバーの目視によって異なるサイバー防御を提供する手法を実装した．システムの検知精度や防御速度ではなく，募集により集めた被験者にアンケートを行い，利便性と安全性についての体感的な判断について調査を行った．本報告書では，この結果について概要を報告する．

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．