# 2013年度 SWAN Working Group 活動報告

宮本大輔 (daisu-mi@nc.u-tokyo.ac.jp)
Gregory Blanc (gregory.blanc@telecom-sudparis.eu)　　門林雄基 (youki-k@is.naist.jp)

2013年12月13日

## 目 次



## 1 はじめに

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．

以降 SWAN WG の本年度の主な活動について報告する．

## 2 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

本研究課題では，ユーザの過去の判断 (Past Trust Decision, PTD) の記録を活用したフィッシングサイト検知を発展させるべく，ユーザのウェブサイトの真贋判定において観測される情報を認知心理学の観点から解析することにより，思考パターンを自動的に判別する方法について検討した．

我々の先行研究 [1] では，ユーザがウェブサイトを見て「正規サイトである」「フィッシングサイトである」という判断を行った結果を，既存のヒューリスティクスを用いたフィッシングサイト検知手法に取り入れることを提案している．昨年度は被験者を募った実験結果を解析し，HumanBoost 方式に適したユーザの傾向として，コンテンツの内容より URL やブラウザのセキュリティ情報に重きをおいて判断している事象が観測され，論文 [2] にまとめた．ただし，これらの判断はアンケート調査を基に採取したものであり，どのよ

うに HumanBoost をシステムとして設計していくかについては今後の検討課題であった．

## 2.1 認知心理学

今年度は，人間が何の情報にもとづいて判断を行っているか，認知心理学の知見を活かして推測する活動を開始した．認知心理学は，思考などの人間の認知活動について研究し，とりわけ人間が学習する課程を解析する学問として知られている．この分野の研究では，人間の活動から観測される様々な生体情報を分析し，人間の思考パターンの変動を予想することが試みられている．生体情報の入手方法は，大掛かりな装置を要するもの，特殊な装置を要するもの，あるいは人体の体内に器具を挿入するものなど様々である．

我々の研究グループでは，人間がコンピュータのユーザであり，ディスプレイ画面を見て操作を行うということを念頭においた検討を行った．検討結果は，人間のミスを防ぐという観点から整理し，論文 [3] として発表した．人間のミスを防ぐ，という目的は直感的には漠然としているものの，研究のアプローチとしては人間がミスを犯す様々な原因を解析し，次なる失敗を起こさないようにするという内容となる．当論文では問題を起こす主体が IT システムのユーザ，場所が家庭や企業における場所，状況が IT システムの利用中と想定した上で，この分野の研究のアプローチを踏襲することとした．

一般的に，失敗の原因は，セキュリティについての知識不足，あるいはその知識を獲得する土壌となるセキュリティ文化・倫理を源泉とし，教育によって解決されるべきものが多い．その一方で，情報セキュリティポリシーなど明確なルールが存在するにも関わらず，別の判断基準を用いて活動を行った結果，ユーザがミスを犯し，インシデントが発生するという事象も考えられうる．例えば，定められた正規の基準を用いず，ユーザがヒューリスティクス（経験則）によりタスクを実行したとしよう．ヒューリスティクスは多くの場合は上手く行くものであり，使用することによって作業時間の劇的な短縮など目に見える効果が得られる．しかし，なぜヒューリスティクスは正規の基準となりえなかったのかを考えれば分かる通り，ヒューリスティクスには上手くいかない場合も存在する．

そこで，時間の短縮のためにヒューリスティクスのような危険な方式を選びそうな状況を判別するべく，ユーザの精神状態の推測を考える．文献 [4] では 4 つの種類の精神状態を定義しており，精神状態は (1) NotKnowing-NotDoing, (2) NotKnowing-Doing, (3) Knowing-NotDoing, そして (4) Knowing-Doing の 4 パターンに分類されている．Knowing はルールを知っているという意味であり，Doing は安全にタスクを実行できるという意味であり，ユーザの心理はこれらの状態を動的に変化している．我々はこの (3) の状態，すなわち教育が有効に効果しているにも関わらず（Knowing），ルールが破られ，安全な行動が実施できない状態（Not-Doing）を観測する方法として，メンタルワークロード（精神的な作業負荷）の変動から観測できないかと考えている．

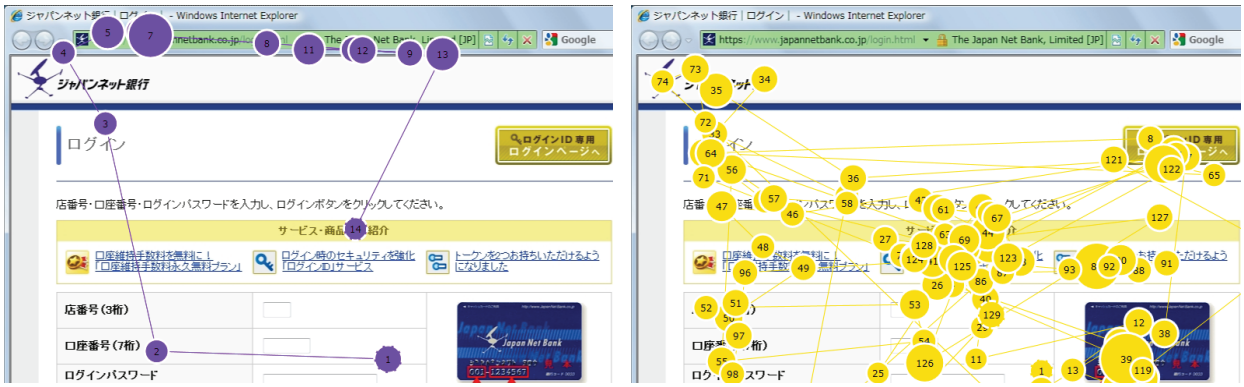
## 2.2 生体情報

メンタルワークロードを推測する情報源となる人間の生体情報には様々な種類がある．ただし，前述の通り IT システムの利用中のミスを想定しているため，要求項目の導出は容易である．論文 [3] では，生体情報に対する機密性に考慮したユースケース，Negative Evaluation [1]を避けるための方策，データを取得する際にその方式がユーザの行動を阻害しないことを掲げている．

例えば，ユーザの表情や行動の類推は Negative Evaluation の影響をうけやすいとされている．また，心拍数や血圧，脳波，呼吸などから類推する方式は Negative Evaluation の影響は受けにくいが，一般的に設備が大掛かりである．もちろん，こうした方式は医療機関においては重要な生体情報取得設備であるが，これらの情報取得を常に行いながら IT システムを利用することは考えにくい．

これらの方式と比較して現実性があるのが視線追跡と顔表面温度による分析ではないかと思われる．とりわけ，視線追跡では眼球運動である衝動性眼球運動，固視，追従眼球運動，前庭動眼反射などの状態を取得している．衝動性眼球運動はサッケードとも呼ばれ，興味をもった点に眼球を動かし視点を移動する眼球運動である．先行研究の事例実験ではサッケード中に意

[1]例えば，苦しいのに笑顔を見せるなどによって，生体情報取得を混乱させるような事象のこと．



(a) 被験者 A の場合　　(b) 被験者 B の場合

図 1: 正規サイト閲覧時の視線計測

思決定は行われることが少なく，精神状態の変化を打ち消す作用があるとされている．また，サッケード中の視線移動速度からメンタルワークロードを推測する試みもなされている．

### 2.3　フィッシングサイト判別への応用

フィッシングサイトを閲覧し，その真贋を判定する場合においても，視線追跡情報を利用できるのではないかと考える．論文 [2] では，HumanBoost 方式に適したユーザの傾向として，コンテンツの内容より URL やブラウザのセキュリティ情報に重きをおいて判断している事象が観測された．視線追跡装置と組み合わせることにより，このユーザが URL やセキュリティ情報を閲覧したかどうかを自動的に判断することができる．すなわち，システムとして設計する上で役立てられると考える．

また，フィッシングサイトを閲覧しているユーザは，果たして普段通りの精神状態であるか否か，といった問題領域についても検討している．例えば，ユーザがフィッシングメールを閲覧し，そのメールに書かれているフィッシングサイトにアクセスするという場合を考える．フィッシングメールは，ユーザをだますべく様々な手法を用いており，卑近な例としてはユーザの利用するサービスで不正が発見されたのでアカウントを凍結した，という内容の文面である．このようなメールに騙されたユーザは，メンタルワークロードが通常の精神状態とは異なり一時的に変動している可能性がある．例えば，ユーザの視線移動速度が通常時と乖離している等の情報からフィッシング攻撃の判定を行えたり，あるいはシステムがユーザに落ち着くよう促したりできる可能性がある．

このような観点から，視線追跡カメラを用い，正規サイトのスクリーンショットを閲覧してもらう事前実験を開始している．図 1(a) はセキュリティに詳しい被験者 A が，図 1(b) はセキュリティに詳しくない被験者 B が正規の銀行ウェブサイトを閲覧した際の視線データである．個々の矢印は視線移動，丸印は固視を示している．被験者 A が URL や SSL の鍵アイコンに注目しているのに対し，被験者 B は画像などのコンテンツに注目している．また，被験者 A の方が被験者 B より閲覧している箇所が少なく，真贋判定基準を保持していると思われる．より多くの被験者を募ってこの実験を行うこと今後の課題である．ただし，フィッシングサイトは正規サイトに似せてつくられているとはいえ，悪性サイトである以上，被験者に直接フィッシングサイトを閲覧させるのは避ける等の対応を適宜とる必要がある．実験倫理に注意した上で実施したい．

## 3　フィッシングサイトのデータセットの Hive 環境への移行の試み

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いる．

```
bin/sqoop import --connect jdbc:postgresql://dbserver/dbname --username username --table pg_table_name -m 1 --direct --direct-split-size 10485854 --hive-import --hive-table hive_tbl_name
```

図 2: Sqoop によるデータ移行の例

これらの研究成果を NECOMA プロジェクトの目標である，他のインシデントとの関連性の分析と突き合わせて解析を行いたい．ただし，データサイズが冗長になることから Apache Hadoop [2]及び Apache Hive [3] を用いることを検討した．

### 3.1 フィッシングサイトのデータベース

フィッシングサイトの取得及びデータについては昨年度の活動記録として論文 [5] にまとめてある．このデータベースは PostgreSQL を採用しており，約 35 万件のフィッシングサイトに関する情報，すなわち URL やドメイン名を複数の DNS サーバで正引きした IP アドレス，ドメイン名を whois により調べた結果，AS 番号といった情報及び報告日が主なレコードである．

### 3.2 Sqoop によるデータ移行

全レコードを Hive に以降する際に，Apache Sqoop [4]の利用を試みた．Sqoop は PostgreSQL のデータに JDBC ドライバを用いて接続し，データの読み書きが行える．図 2 にデータ移行の例を示す．任意のデータベースのテーブル `pg_table_name` を読み取り，Hive 上のテーブル `hive_tbl_name` へのデータのインポートを行っている．また，プライマリキーや HDFS 上にファイルを設置する際の分割サイズも指定することができる．

設置したデータの活用は課題であるが，例えば NECOMA プロジェクトにおいて発見したボットネットや外部のボット関連情報のリソースと，IP アドレスを相互に参照するなどの方法を考えている．

[2] http://hadoop.apache.org
[3] http://hive.apache.org
[4] http://sqoop.apache.org

## 4 おわりに

本年度の SWAN Working Group の活動は，悪性ウェブサイトの 1 つであるフィッシングサイトに焦点を当て，また WIDE の幅広い人脈を活かし，認知心理学の活用や他のインシデントとの解析のための準備を行った．来年度も幅広い種類の悪性ウェブサイトについて，多面的な解析を行うことが課題である．

## 参考文献


[1] Daisuke Miyamoto, Hiroaki Hazeyama, Youki Kadobayashi, *"HumanBoost: Utilization of Users' Past Trust Decision for Identifying Fraudulent Websites,"*, *Journal of Intelligent Learning Systems and Applications*, Vol. 2, No. 4, pp.190-199, December 2010.

[2] Daisuke Miyamoto, Hiroaki Hazeyama, Youki Kadobayashi, Takeshi Takahashi, *"Behind HumanBoost: Analysis of Users' Trust Decision Patterns for Identifying Fraudulent Websites,"*, *Journal of Intelligent Learning Systems and Applications*, Vol. 4, No. 4, pp.19-329, November 2012.

[3] Daisuke Miyamoto, Takeshi Takahashi, *"Toward the Automated Reduction of Human Errors based on Cognitive Analysis,"*, *In Proceedings of the 7th International Workshop on Advances in Information Security*, July 2013.

[4] Salahuddin Alfawaz, Karen Nelson, Kavoos Mohannak, *"Information security culture: a behaviour compliance conceptual framework,"*, *In Proceedings of the 8th Australasian Conference on Information Security*, July, 2010.

[5] Daisuke Miyamoto, Yuzo Taenaka, Toshiyuki Miyachi, Hiroaki Hazeyama, *"PhishCage: Reproduction of Fraudulent Websites in the Emulated Internet,"*, *In Proceedings of the 1st Workshop on Emulation Tools, Methodology and Techniques*, March 2013.