Vol.2017-MPS-115 No.1
2017/9/25

潜在曲線モデルによるWireshark操作スキル推定

松田 健[1,a)]　園田 道夫[†1]　衛藤 将史[†1]　佐藤 公信[†1]　花田 智洋[†1]　金濱 信裕[†1]　石川 大樹[†1]

概要：ICT 技術の活用場面が増えれば増えるほど，新たなセキュリティリスクも増加すると考えられるため，既存の脅威のみならず，未知の脅威にも対処することができるセキュリティ人材の育成が課題となっている．そのためには，高度な技術をもつ指導者が必要であるが，それぞれの学習者のスキルを適切に把握することが出来れば，効率の良い技術の教授が可能となると考えられる．そこで本研究では，ネットワーク上のデータをキャプチャーするためのツールである Wireshark の操作画面をデスクトップごとキャプチャーし，その画像を解析することで操作をしている技術者のスキルを潜在曲線モデルにより推定する方法を提案する．

Skill Estimation of Wireshark Operation by Latent Curve Analysis

Matsuda Takeshi[1,a)]　Sonoda Michio[†1]　Etou Masashi[†1]　Satoh Hironobu[†1]
Hanada Tomohiro[†1]　Kanahama Nobuhiro[†1]　Ishikawa Daiki[†1]

1. はじめに

ICT 技術の発展により，現在では生活の様々な場面でインターネットを活用したサービスが利用されるようになっている．インターネット上では個人のショッピングや組織間の機密情報のやり取りなど，様々なデータのやり取りが行われているため，このようなデータはサイバー攻撃の攻撃者の標的になっている．今後は，IoT 技術を活用したサービスも展開されていくことを考えると，新たなサイバー攻撃の出現にも対応出来る技術者の育成も急務であると言える．実際，厚生労働省の報告 [1] によると，2020 年には 19.3 万人のセキュリティ人材が不足するであろうと予測されており，それに向けた人材育成事業も進められている [2]．本研究では，このような人材育成に関わる教育コンテンツに対して，ICT 技術を活用した切り口で教材を開発する手法について検討する．具体的には，ネットワークを流れるデータをキャプチャーして解析することが出来る Wireshark[3] を用いて，Wireshark の操作スキルを持つユーザーと持たないユーザーのデスクトップ上の操作画面を動画で記録して，スキルを持つユーザーとそうでないユーザーにどのような違いがあるかということについて検討する．Wireshark はネットワーク上のデータの監視に利用できるため，セキュリティに関連する問題解決にも有用であると言えるため，本研究では，デスクトップ操作画面の動画データからユーザーのスキルを推定する方法を提案する．動画データは 5fps で取得し，時刻 t と $t+s$ の画像の RGB 値の差分が一定以上の値となる 2 つの画像データを選択し，この 2 つの画像データを 120×160 のサイズに縮小してユーザーの作業内容を推定するための特徴を生成する．ただし，t, s は自然数である．本研究では，Wireshark の操作経験を持つユーザー 2 人と，ほとんど操作経験の無いユーザー 3 人のデータを取得し，潜在曲線モデルの手法を応用することでこれらのユーザーがどのような作業を行っているかを推定した．Wireshark は非常に多くの機能が実装されており，そのすべての機能の使い方をデータとして取得することは困難であると考えられる．そこで本研究では，デスクトップ上の作業内容をカーソル移動のみ，スクロールのみ，Wireshark の機能使用の 3 つの作業に分類し，キャプチャーした動画データから作業内容を推定する方法を提案した．

[1] 長崎県立大学
Nagayo, Nishisonogigun, Nagasaki, 851–2195, Japan
[†1] 現在，情報通信研究機構
[a)] tmatsuda@sun.ac.jp

ⓒ 2017 Information Processing Society of Japan

2. 従来研究

Wireshark を使用すると，Wireshark を起動している端末から外部のネットワークに流れる出るデータや，その端末に入ってくるデータをキャンプチャーして分析することができるため，Wireshark はネットワークやセキュリティに関する様々な問題解決のためのツールとして広く利用されている．図 1 は Wireshark の操作画面である．キャプチャーした pcap(拡張子) ファイルに含まれるデータが大量である場合は，送信元の IP アドレス，HTTP や TCP/IP などのプロトコルのみのデータが閲覧できるようなフィルタ機能を使用したり，ダウンロードされたファイルをエクスポートしたりする機能を利用して解析すると作業効率が向上する．Wireshark は非常に多くのプロトコルに対応しているが，対応していないプロトコルの場合は，Lua を用いて自由に新たな機能を開発することが出来る．例えば文献 [4] では，日本電気工業会の PMCN(Protocol for Mission Critical industrial Network use) と呼ばれるプロトコルを解析する手法が紹介されている．また，Wireshark の機能を用いたサイバー攻撃に対する防御方法についても研究されており，文献 [5] では，パケット解析に基づいた DDoS 攻撃の対策について検討されている．また，文献 [6] では，ネットワークカメラに対するパケットデータの解析方法について紹介されている．ここで紹介した研究以外でも，Wireshark の機能を応用する研究は多数存在するが，ユーザーの操作データを解析する研究はこれまでに発表されていない．また，セキュリティ教育に関する論文についても，文献 [7] のように仮想的なネットワークをソフトウェアで作成してネットワークセキュリティ教育を行う手法や，文献 [8] のように攻撃手法について解説する書籍が多く，高い技術力を持つ技術者が具体的にどのように作業をしているかということを教材に活用する研究は見受けられない．そのようなコンテンツは動画公開サイトの YouTube に存在する可能性はあるが，どのコンテンツが良いコンテンツであるかということを効率良く調べる方法についても，まだ多くの知見があるとは言えない状況である．そこで本研究では，ユーザーのデスクトップ画面をキャプチャーして，ユーザーが Wireshark のどのような機能をどのように使用しているか画像データから推定し，操作スキルを持つユーザーと持たないユーザーでどのような差が見られるかということについて考察した．なお，本研究では，WindowsOS 上で Wireshark を使用しているため，専用のツールを利用すれば，ユーザーのキーボード入力やマウスの移動データを取得することも可能である．しかしながら，キーボード入力やマウスの動き方だけではどのような作業をしているか特定することが困難である場合も確認できたため，本研究ではデスクトップの画像を解析することで，ユーザーの作業内容を推定する手法の開発を目指す．

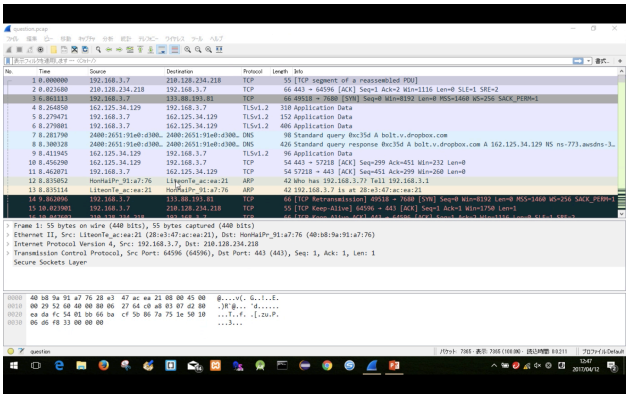

図 1　Wireshark の操作画面

3. 提案手法

3.1 分析データの生成

本研究では，Wireshark の操作画面の動画データから，ユーザーがどのような作業をしているか推定する手法を提案する．ユーザーには，あるソフトウェアをダウンロードしているときの pcap ファイルと，あるサイバー攻撃が行なわれているときの pcap ファイルを用意し，Wireshark の操作経験を持つユーザー 2 人と，操作経験がまったくないか，もしくはほとんどないユーザー 3 人のデータを取得した．なお，動画データは 5fps で記録しているが，ユーザーや作業内容によってはデスクトップ画面に変化が見られない場面をあるため，時刻 t と $t+s$ の画像データの RGB 値の差分をとって，その値がある閾値を超えた場合に 2 つの画像 I_t と I_{t+s} を取得してデータの分析に利用した．なお，閾値については全ユーザーが共通の値の場合は，データがまったく取れないこともあるため，作業内容が把握できるレベルで逐次更新してデータを取得している．例えば，カーソルを移動させるだけの作業の場合は，画像全体における RGB 値の変化が少ないため，閾値を固定すると「カーソル移動」という作業内容を取得できなくなる場合が存在するため，閾値を固定せずにデータを生成した．このようにして，デスクトップ操作の動画データから画像データを生成し，取得した順番にナンバリングし直して，画像データの集合

$$\mathbf{I} = \{I_1, I_2, \cdots\}$$

を生成する．なお，画像データのサイズは 120×160 (height $\times$ width) とし，2 つの画像 I_i, I_{i+1} の絶対値差分からなる 120×160 行列を生成して，それぞれの行方向と列方向の総和の値を計算してできる 280 次元ベクトルを構成した．さらに，この 280 次元ベクトルの成分を 20 個ずつの 14 個の領域に分けて，それぞれの領域において 280 次元ベクトルの各成分の値が 200 を超えている成分の個数をカウントし

ⓒ 2017 Information Processing Society of Japan

て 14 次元ベクトルを生成した．以下，このようにして生成されたデータの集合 $\mathbf{D}$ を以下のように表すことにする．

$$\mathbf{D} = \{\mathbf{d}_1, \mathbf{d}_2, \cdots\},$$

ただし，$\mathbf{d}_i = (d_{1i}, d_{2i}, \cdots, d_{14i})$ とする．図 2 は 14 次元ベクトルの散布図である．この散布図の横軸の 1 ～ 14 は 14

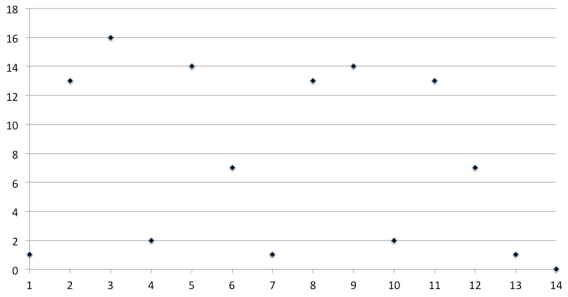

図 2　分析用データの散布図

次元ベクトルの j 番目 $(1 \leq j \leq 14)$ の成分に対応する．本研究で取得したデータは図 2 のように散布図の中心付近でピッタリではない場合もあるが，左右対称であるため，実際の分析には 14 次元ベクトルのうち初めの 6 次元ベクトルを使用した．したがって，これ以降は

$$\mathbf{d}_i = (d_{1i}, d_{2i}, \cdots, d_{6i})$$

として扱うことにする．

3.2　提案モデル

本研究の目的は，Wireshark の操作動画データからユーザーのスキルを評価する方法について検討することであるが，そのために，動画データから Wireshark のどのような機能を利用しているかということを推定して，その結果を用いてユーザーのスキルの特徴について考察する．Wireshark に標準で用意されている機能は多数存在するため，特定の機能を全て分類することは困難である．そこで本研究では，大雑把な作業内容にデータを分類してそれを推定する方法について検討する．具体的には，

・カーソル移動
・スクロール
・機能使用

の 3 つの状態に動画データを分類する方法について検討する．今回取得したデータ数は動画の総時間の合計は 30 分程度に及ぶが，以下の表 1 に示す通り，カーソル移動やスクロール，機能使用のデータのパターンはほとんど同じようなものになるため，少ないデータの個数で作業内容を分類可能なモデルの構成を目指した．

デスクトップでの作業内容を推定するモデルとして，以下の 4 次関数からなるモデルを提案する．

$$y_x = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0, \qquad (1)$$

表 1　取得したデータの一部

状態	データ
カーソル移動 1	(0,3,4,0,0,0,1,0,0,3,4,0,0,0,0)
カーソル移動 2	(0,0,0,3,0,0,1,0,0,0,0,3,0,0,0)
スクロール 1	(0,18,20,6,0,0,1,0,0,18,20,6,0,0,0)
スクロール 2	(0,3,5,3,0,0,1,0,0,4,7,4,0,0,0)
機能使用 1	(1,13,16,2,14,7 1,13,14,2,13,7,1,0,0)
機能使用 2	(0,2,8,0,0,0,0,2,8,0,0,0,1,0,0)

ただし，$x = 1, 2, \cdots, 6$ であり，$a_0, a_1, a_2, a_3, a_4 \in \mathbf{R}$ とする．また，y_x は 6 次元ベクトル $\mathbf{d}_i$ の x 番目の成分の値である．パラメータ a_0, a_1, a_2, a_3, a_4 については $y - (a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0)$ の誤差が平均 0 の正規分布に従うと仮定した上で，最尤推定法を適用して推定することにする．これにより，パラメータの学習が上手くできていれば，a_0, a_1, a_2, a_3, a_4 の値は x, y_x の関数として表現されるため，対応するデータの状態 (カーソル移動，スクロール，機能使用) によってパラメータの値に応じて分類されているものと考えられる．そこで，状態を表す潜在変数 $s \in \{0, 1\}$ を導入して，

$$a_j = p_js + b_j \qquad (2)$$

という線形なモデルを用意して，潜在変数 s に関連するパラメータ p_j, s_j $(j = 0, 1, 2, 3, 4)$ を，誤差 $a_j - (p_js + b_j)$ が平均 0 の正規分布に従うと仮定して最尤推定法により推定する．

4.　実験と結果

前章で提案したモデルに対してデータを適用し，ユーザーの作業内容を推定した結果についてまとめる．表 1 に示したデータの傾向から，カーソル移動とそれ以外の状態については明確に分類できることが期待できる．しかしながら，Wireshark の機能使用とスクロールについては，前述のような傾向があるとは言い難いと考えられる．そこで，データを 3 値に分類するのではなく，

・カーソル移動とそれ以外（実験 1）
・機能使用とそれ以外（実験 2）

の 2 つのパターンに分類可能であるか検討した．

4.1　実験 1

提案モデル (1), (2) 式のパラメータ a_0, a_1, a_2, a_3, a_4 に与えた潜在変数 s に対して，カーソル移動をしている状態を $s = 1$，それ以外の状態を $s = 0$ と定義して，$s = 1$ であるデータを 15 個，$s = 0$ であるデータを 18 個用意して (2) 式のパラメータ p_j, b_j (j=0, 1, 2, 3, 4) を推定した結果を表 2 にまとめる．

これにより，$s = 1$ である場合，つまりカーソル移動をしている状態の特徴を (1) 式により図 3 のように表現することができる．図 3 の曲線の方程式は

表 2　カーソル移動とそれ以外のデータ学習の結果

a_4	$p_4 = 0.118981481$	$b_4 = -0.023148148$
a_3	$p_3 = -1.345164602$	$b_3 = 0.380658439$
a_2	$p_2 = 2.68996915$	$b_2 = -2.279321006$
a_1	$p_1 = 8.028718219$	$b_1 = 5.642269299$
a_0	$p_0 = -7.040740604$	$b_0 = -3.703703733$

$$y_x = 0.096x^4 - 0.964x^3 + 0.411x^2 + 13.671x - 10.744$$

である．同様に，図 4 はカーソル移動以外の状態の特徴を

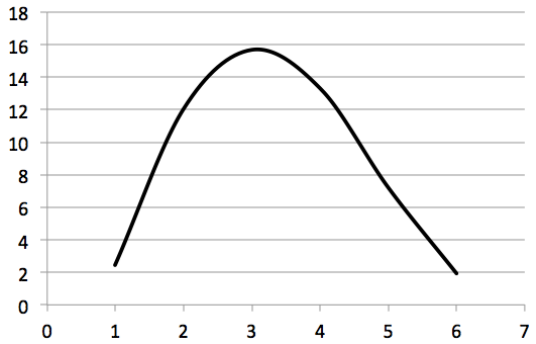

図 3　カーソル移動の特徴

示している．図 4 の曲線の方程式は

$$y_x = -0.023x^4 + 0.381x^3 - 2.279x^2 + 5.642x - 3.704$$

である．

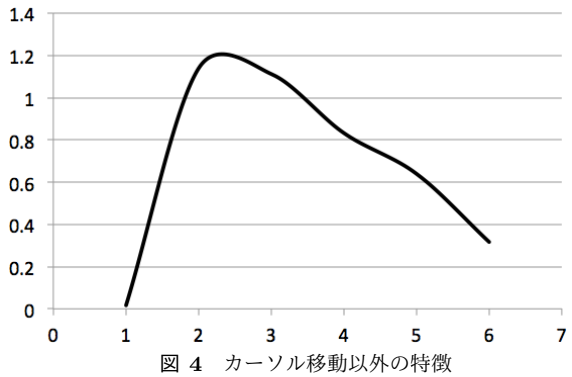

図 4　カーソル移動以外の特徴

パラメータの学習に使用したデータ以外のデータを 15 個用意し，どちらの曲線にフィッティングするかということを計算してデータの分類を行ったところ，表 3 の結果が得られた．

4.2　実験 2

機能使用の状態を $s = 1$，それ以外の状態を $s = 0$ と定義して，実験 1 と同じく $s = 1$ であるデータを 15 個，$s = 0$ であるデータを 18 個用意して (2) 式のパラメータ p_j, b_j (j=0, 1, 2, 3, 4) を推定した結果を表 4 にまとめる．

表 3　カーソル移動とそれ以外のデータ学習の結果

真のラベル	推定結果
カーソル移動	カーソル移動
カーソル移動	カーソル移動
カーソル移動	カーソル移動
カーソル移動	カーソル移動
カーソル移動以外 (スクロール)	カーソル移動以外
カーソル移動以外 (スクロール)	カーソル移動以外
カーソル移動以外 (スクロール)	カーソル移動以外
カーソル移動以外 (スクロール)	カーソル移動以外
カーソル移動以外 (スクロール)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外

表 4　カーソル移動とそれ以外のデータ学習の結果

a_4	$p_4 = 0.055324073$	$b_4 = 0.005787037$
a_3	$p_3 = -1.154475302$	$b_3 = 0.293981484$
a_2	$p_2 = 6.686805562$	$b_2 = -4.096064848$
a_1	$p_1 = -11.76529997$	$b_1 = 14.63955038$
a_0	$p_0 = 8.338888998$	$b_0 = -10.69444453$

これにより，$s = 1$ である場合，つまりカーソル移動をしている状態の特徴を (1) 式により図 3 のように表現することができる．図 3 の曲線の方程式は

$$y_x = 0.061x^4 - 0.860x^3 + 2.591x^2 + 2.674x - 2.356$$

である．同様に，図 4 はカーソル移動以外の状態の特徴を

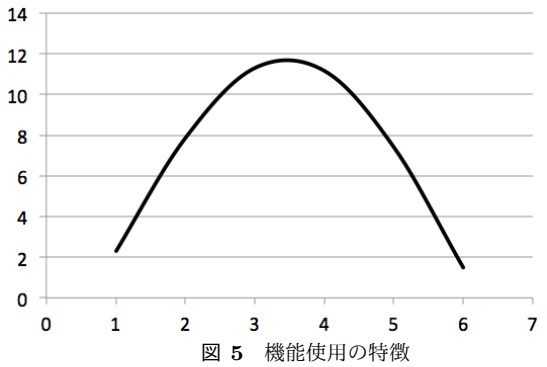

図 5　機能使用の特徴

示している．図 4 の曲線の方程式は

$$y_x = 0.006x^4 + 0.294x^3 - 4.096x^2 + 14.640x - 10.694$$

である．

パラメータの学習に使用したデータ以外のデータを 15 個用意し，どちらの曲線にフィッティングするかというこ

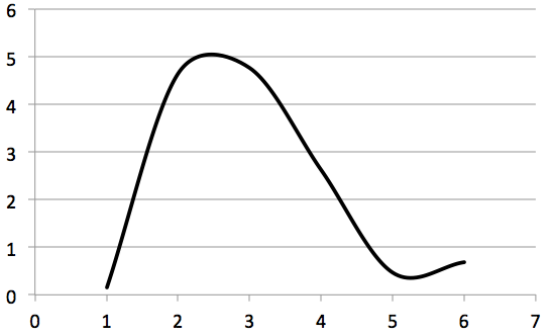

図 6　機能使用以外の特徴

とを計算してデータの分類を行ったところ，表 3 の結果が得られた．

表 5　カーソル移動とそれ以外のデータ学習の結果

真のラベル	推定結果
カーソル移動	カーソル移動
カーソル移動	カーソル移動
カーソル移動	カーソル移動
カーソル移動	カーソル移動
カーソル移動以外 (スクロール)	カーソル移動
カーソル移動以外 (スクロール)	カーソル移動
カーソル移動以外 (スクロール)	カーソル移動以外
カーソル移動以外 (スクロール)	カーソル移動以外
カーソル移動以外 (スクロール)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外
カーソル移動以外 (機能使用)	カーソル移動以外

4.3　ユーザーのスキル評価について

本研究では，Wireshark の操作経験を持つユーザー 2 人と，操作経験がまったくないか，もしくはほとんどないユーザー 3 人のデータを取得して，ユーザーがどのような作業をしているか分類する手法を提案した．操作経験の無いユーザーは大抵の場合はカーソルを移動させるか画面をスクロールしているだけのデータが多いが，稀に Wireshark の機能を利用する場面もみられた．その際にウィンドウが表示されるが，すぐに開かれたウィンドウを閉じてまたカーソル移動や画面のスクロールをするという傾向が見受けられた．一方で，操作経験のあるユーザーもカーソル移動やスクロールだけをしている時間はあるが，ある程度問題解決の方針が固まると今度は Wireshark の機能を使用したり，その他の WindowsOS の機能を利用したりする傾向が見受けられた．実験 1 と 2 の結果から，カーソル移動・スクロール・機能使用の 3 つの状態はおおまかに分類できることが確認できるため，本研究で取得したデータについては上述の特徴を考慮することで，Wireshark の操作経験の有無を評価する程度の推定を行うことは可能であるといえる．

5.　結び

本研究では，Wireshark の操作画面の動画データから，ユーザーがどのような作業をしているか推定する手法を潜在曲線モデルの手法を応用して提案した．今後の課題は，より多くのデータを取得した場合でも高精度に作業内容を推定し，ユーザーのスキル評価を行う手法を開発することで，データを活用した教育コンテンツの開発に繋げることである．

参考文献

[1] 経済産業省：“IT 人材の最新動向と将来推計に関する調査結果を取りまとめました”，(online)，入手先 ⟨http://www.meti.go.jp/press/2016/06/20160610002/20160610002.pdf⟩ (2017.08.25).
[2] SecHack365-セキュリティの未来を生み出す U-25 ハッカソン-(online)，入手先 ⟨https://sechack365.nict.go.jp/⟩ (2017.08.25).
[3] Wireshark(online)，入手先 ⟨https://www.wireshark.org/download.html⟩ (2017.08.25).
[4] 小島 一浩, 天雨 徹：Wireshark 用 Lua Dissector を活用した PMCN 解析手法, 電気学会研究会資料. PPR 2015(1-24), pp.111-114 (2015).
[5] Waqar Ali, Jun Sang, Hamad Naeem, Rashid Naeem, Ali Raza.: *Wireshark window authentication based packet captureing scheme to pervent DDoS related security issues in cloud network nodes*, 2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp.114-118 (2015).
[6] Resul Das, Gurkan Tuna.: *Packet tracing and analysis of network cameras with Wireshark*, 2017 5th International Symposium on Digital Forensic and Security (ISDFS), pp.1-6 (2017).
[7] Jun Wu, Shen Wang, Jianhua Li, Yang Wu.: *SDSEP: A Network Security Education Platform Based on Software-Defined Networking Technology*, 2016 8th International Conference on Information Technology in Medicine and Education (ITME), pp. 737 - 740 (2016).
[8] Dan Chia-Tien Lo, Kai Qian; Wei Chen.: *Hardware Attacks and Security Education*, 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Volume: 2, pp. 253 - 257 (2016) .

ⓒ 2017 Information Processing Society of Japan