Computer Security Symposium 2020
26 - 29 October 2020

URLバーの切り替わり間隔に着目した意図しないWebサイト遷移の検知手法の改善と実証実験データによる評価

折戸 凜太郎[1]　佐藤 将也[1]　梅本 俊[2]　中嶋 淳[2]　山内 利宏[1]

概要：Android において，リダイレクトにより利用者の意図しない Web サイト（以降，悪性 Web サイト）へ誘導する攻撃が存在する．この攻撃への対策として，我々は，アクセシビリティサービスを用いた URL バーの切り替わり間隔に着目した悪性 Web サイトへの遷移を検知する手法（以降，提案手法）を提案した．また，実際の Android 端末の利用を想定した環境において実施した評価より，提案手法の悪性 Web サイトへの遷移と判定する URL バーの切り替わり回数や経過時間の閾値を設定した．しかし，ここで閾値を設定するにあたり誤検知の削減を優先したため，誤検知率は非常に低い値となったものの，見逃し率は高い値となってしまい悪性 Web サイトを検知する手法としては十分ではなかった．本研究では，良性 Web サイトの誤検知率を抑制しながら，悪性 Web サイトの見逃し率を削減できる改善手法を提案し，その評価について述べる．また，スマートフォンを対象にしたユーザ参加型 Web 媒介型攻撃対策の実証実験において，参加者端末にインストールするアプリに提案手法を実現し，実証実験で収集したデータで評価し，有効性について述べる．

Improvement for Detection Method of Transition to Unwanted Website Focusing on URL Bar Switching Interval and Evaluation using Data of Demonstration Experiment

Rintaro Orito[1]　Masaya Sato[1]　Shun Umemoto[2]　Jun Nakajima[2]　Toshihiro Yamauchi[1]

Abstract: There is an attack that redirects an user to an unwanted website in Android. To take measure to this attack, we have proposed detection method of transition to unwanted website focusing on URL bar switching interval using the accessibility service. In addition, we set the thresholds of the proposed method for number and elapsed time of URL bar switches which determine whether a transition to an unwanted website or not. In the above setting the thresholds, we prioritized reduction of false positives. Therefore, although the false positive rate is low, the false negative rate is high, which the proposed method is not good performance as a method for detecting malicious websites. In this paper, we describe improvement for the proposed method to reduce the false negative rate while maintain the false positive rate. In addition, we describe the evaluation of the proposed method using the data of the demonstration experiment.

1. はじめに

Android において利用者の意図しない Web サイト（以降，悪性 Web サイト）へ誘導する攻撃が存在する．この攻撃では，利用者が誘導元の Web サイト（以降，遷移元サイト）へ Web アクセスした際，自動的もしくは画面のタップなどの操作を契機として発生するリダイレクトにより，複数の Web サイト（以降，経由サイト）を経由した後に目的の悪性 Web サイトへ誘導する．この攻撃の複数の Web サイトを経由する点は，文献 [1] で述べられている Drive-by

[1] 岡山大学 大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
[2] 株式会社セキュアブレイン
SecureBrain Corporation

Download 攻撃と類似している．しかし，Android 端末は PC とは異なり，利用者の許可なくソフトウェアを自動的にインストールできない．このため，この攻撃では，誘導先の Web サイトにて様々な手口により利用者を欺くことで，広告収入の獲得や個人情報の奪取を目的としている [2]．たとえば，悪性 Web サイトには偽警告画面を表示する Web サイトやフィッシングサイトなどがあり，これらの Web サイトでは偽警告や偽懸賞当選を表示する [3]．

この対策として，URL やドメイン名のブラックリストを用いる手法がある．しかし，悪性 Web サイトは多数存在することに加えて，URL とドメイン名は短期的に変更される特徴がある [3]．また，ある URL から HTTP Alternative Services により別の URL へリダイレクトする際，Google Safe Browsing ではリダイレクト前の URL のみを検査しており，リダイレクト先の URL が検知対象であっても Web アクセスが防止されない [4]．以上より，この手法により悪性 Web サイトへの遷移を防止することは難しい．

また，リダイレクトによって複数の経由サイトを経由する特徴に着目した先行研究がある [1], [5]．しかし，これらの研究は Android を対象としていない．また，我々が調査した限りでは，上記の先行研究を含め，Android を対象とした悪性 Web サイトへ誘導する攻撃への対策を提案している研究はない．

そこで，我々は，Android を対象とする Web 上で利用者を悪性 Web サイトへ誘導する攻撃への対策として，Android のアクセシビリティサービスを用いた URL バーの切り替わり間隔に着目した利用者の意図しない Web サイトへの遷移を検知する手法（以降，提案手法）を実現した [6]．提案手法は，悪性 Web サイトへ遷移する際の複数のリダイレクトの発生する間隔に着目して，悪性 Web サイトへの遷移を検知する手法である．

また，提案手法の悪性 Web サイトへの遷移と判定する URL バーの切り替わり回数や経過時間を適切に設定するため，良性 Web サイトと悪性 Web サイトを用いた評価を実施した [7]．ここでは，良性 Web サイトと悪性 Web サイトにおいてリダイレクトが発生した際の URL バーの切り替わり回数や経過時間を評価した結果に基づいて閾値を設定した．しかし，閾値を設定するにあたり，利便性を考慮して悪性 Web サイトの見逃しを抑制することよりも良性 Web サイトの誤検知を抑制することを優先した．これにより，誤検知率は非常に低い値となったものの，見逃し率は高い値となってしまい悪性 Web サイトを検知する手法としては十分ではない．

そこで，本研究では，良性 Web サイトの誤検知率を抑制しながら，悪性 Web サイトの見逃し率を削減するための改善手法を提案する．この手法は，ユーザ操作のリンクのタップ操作に着目して，良性 Web サイトへのアクセスを検知対象から除外する．また，「戻る」操作を連続操作される場合も，判別し，検知対象から除外する．さらに，ホワイトリストを導入し，Alexa Top Site などを調査し，誤検知を削減する．本稿では，改善手法の検知精度の評価結果より，改善前と比較して，誤検知を増やさずに提案手法の見逃しを大幅に削減できることを示す．

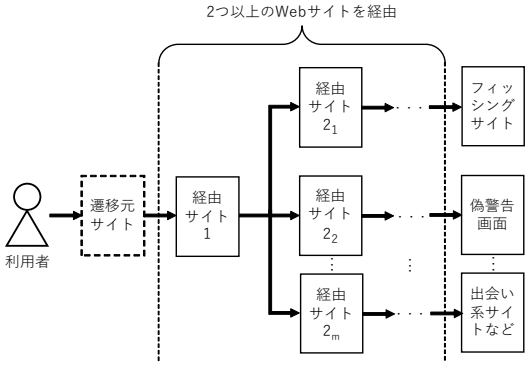

図 1 悪性 Web サイトへの遷移の流れ [6]

さらに，Web 媒介型攻撃対策技術の実用化に向けた研究開発（WarpDrive）[8] では，スマートフォンを対象にしたユーザ参加型の Web 媒介型攻撃観測システムを提案している [9]．このシステムでは，参加者端末にインストールするセンサアプリより，Web アクセスなどのデータ（以降，実証実験データ）を収集して，これらを分析に利用する．本稿では，改善した提案手法を実装したセンサアプリにより収集した実証実験データを用いた評価について述べる．

2. 利用者の意図しない Web サイトへの遷移の検知手法

2.1 利用者の意図しない Web サイト

文献 [10] では，悪性 Web サイトの 1 つである偽警告画面を表示する Web サイトへの遷移の特徴を明らかにしている．また，その後の調査により，偽警告画面を表示する Web サイト以外への遷移であっても同様の特徴がみられることを明らかにしている [6]．

ここで明らかにした遷移元サイトから悪性 Web サイトへの遷移の流れを**図 1** に示す．この遷移の特徴として，図 1 に示すよう，悪性 Web サイトへはリダイレクトにより 2 つ以上（多くの場合，3 つ以上）の経由サイトを経由した後に誘導される．また，経由サイトでは Web アクセスするごとに異なる URL を生成して，生成した URL をリダイレクト先とする．これにより，攻撃が実行されるごとに URL が異なる次の経由サイトへ遷移して，経由サイトの URL や誘導先の悪性 Web サイトの種類は攻撃が実行されるごとに変化する．

2.2 提案手法

我々は，Android における利用者を悪性 Web サイトへ誘導する攻撃への対策として，URL バーの切り替わり間

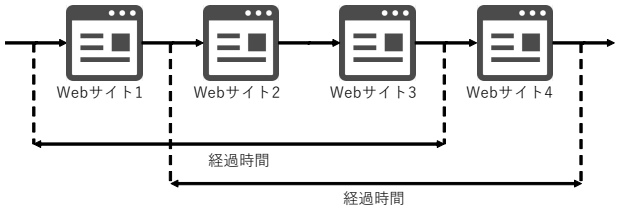

図 2 経過時間の算出方法

隔に着目した利用者の意図しない Web サイトへの遷移を検知する手法を実現した [6]．なお，提案手法の監視対象 Web ブラウザは，Google Chrome である．

提案手法は，Web ブラウザが Web アクセスしたことを監視するため，アクセシビリティサービスにより Web ブラウザの URL バーの切り替わりを監視する．アクセシビリティサービスは，画面上の状態を観測して，その観測した状態に対して多くのサービスを提供する．Google Chrome では，Web サイトが切り替わるごとに URL バーに表示されている URL の内容が変化する．このため，URL バーの内容変化を示すイベントが発生した際，Web サイトが切り替わったと判別する．

また，悪性 Web サイトへ遷移する際，リダイレクトが短時間のうちに連続して発生することから，URL バーの内容変化を示すイベントも短時間のうちに連続して発生する．このため，このイベントが一定時間内に連続して発生した際，悪性 Web サイトへ遷移したと判定する．

以上より，提案手法は以下の 2 つの閾値に基づいて悪性 Web サイトへの遷移を検知する．

(閾値 1) 経過時間の算出に用いる URL バーの切り替わり時刻（何回前の時刻であるかを指定）

(閾値 2) 悪性 Web サイトへの遷移と判定する経過時間

提案手法が悪性 Web サイトへの遷移を検知する様子を**図 2** に示す．提案手法は，図 2 に示すよう，URL バーの切り替わりが発生するごとに数回前（閾値 1）の切り替わり発生時刻からの経過時間（閾値 2）を算出する．経過時間が設定した閾値よりも短い場合，悪性 Web サイトへ遷移していると判定する．なお，図 2 は，3 回前の URL バーの切り替わり時刻から経過時間を算出している例（(閾値 1) を 3 回と設定している例）を示している．

2.3 提案手法の問題点

文献 [7] では，良性 Web サイト，および悪性 Web サイトを用いた評価を実施して，その評価結果を基に提案手法の（閾値 1）を「3 回」，（閾値 2）を「4,000ms」に設定した．ここで閾値を設定するにあたり，利便性を考慮して悪性 Web サイトの見逃しを抑制することよりも良性 Web サイトの誤検知を抑制することを優先した．これにより，**表 1** に示すよう評価を実施した 3 つの環境のすべてにおいて誤検知率は低い値となった．しかし，誤検知を抑えることを優先して（閾値 2）を短い値に設定したため，見逃し率は高い値となってしまい，悪性 Web サイトを検知する手法としては十分ではない．以上より，良性 Web サイトの誤検知率を抑制しながら，悪性 Web サイトの見逃し率を削減する方法を検討する必要がある．

表 1 改善前の提案手法の検知精度 [7]

	(A) Wi-Fi (岡山大学)	(B) IIJ	(C) Y!mobile
誤検知率	12%	5.9%	5.9%
見逃し率	44%	67%	61%

3. 提案手法の改善

3.1 目的と考え方

本研究の目的は 2.3 節で述べた問題点へ対処するため，提案手法の良性 Web サイトの誤検知率を抑制しながら，悪性 Web サイトの検知率を向上させることである．悪性 Web サイトの検知率は，（閾値 2）を長く設定することで容易に向上できると推察する．しかし，このとき良性 Web サイトの誤検知率が増加する [7]．ここで，閾値を変更する他に良性 Web サイトを判別できる場合，（閾値 2）を長く設定しても誤検知率を抑制でき，悪性 Web サイトの検知率を向上できると推察する．そこで，良性 Web サイトと悪性 Web サイトの特徴の違いに着目して，良性 Web サイトを判別する手法を検討する．

3.2 課題

良性 Web サイトへの遷移と悪性 Web サイトへの遷移の特徴の違いとして，直前のユーザ操作がある．たとえば，良性 Web サイトの場合，遷移の直前にはリンクを含むコンテンツのタップなどのユーザ操作が実行されることが多い．一方，悪性 Web サイトの場合，遷移元サイトにおいて遷移の契機となるタップが 1 回実行されるのみであり，その後はリダイレクトにより遷移する．このため，リンクを含むコンテンツのタップなどのユーザ操作を検知することで，ほとんどの良性 Web サイトへの遷移を判別できると推察する．以上より，3.1 節で述べた目的を達成するために以下の 3 つの課題に対処する．

(課題 1) リンクのタップを検知する方法の検討

良性 Web サイトにおいて，リンクのタップにより短い間に連続して Web サイトを切り替えることで誤検知が発生する可能性がある．悪性 Web サイトへ遷移する際は，リダイレクトにより Web サイトが切り替わる．一方，良性 Web サイトでは，多くの場合，リンクをタップした後に Web サイトが切り替わる．このため，リンクのタップを検知できた場合，良性 Web サイトと悪性 Web サイトを判別できると推察する．

(課題 2) 「戻る」操作を検知する方法の検討

「戻る」操作を連続で実行した際，短い間に連続して

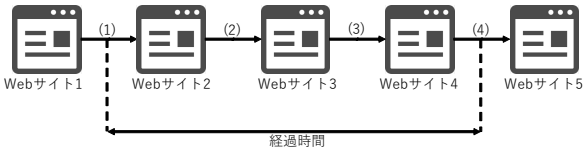

図 3 リンクのタップによる誤検知への対処

Web サイトが切り替わるために誤検知が発生する可能性がある．Android では，この「戻る」操作を実行するためには，「戻るボタン」を押下する必要がある．このため，この「戻るボタン」の押下を検知できた場合，「戻る」操作による Web サイトの切り替わりを判別できると推察する．

(課題 3) その他の操作による遷移を検知する方法の検討

リンクのタップや「戻る」操作以外のユーザ操作により URL バーが切り替わる場合がある．たとえば，Google Map の URL は地図の中心の座標とズームレベルで構成されており，地図をスライド，拡大縮小すると URL が変化する．この操作は，連続して実行でき，これにより URL バーの内容が短い間に連続して切り替わるため誤検知が発生する可能性がある．このため，特定の操作による誤検知へ対処する必要がある．

3.3 課題への対処

3.3.1 （対処 1）リンクのタップを検知する方法

リンクを含むコンテンツをタップした際，アクセシビリティサービスにより観測できるイベント “TYPE_VIEW_CLICKED” が発生する．このため，このイベントを観測して，これが発生した直後の Web サイトの切り替わりをリンクのタップによる切り替わりとする．

図 3 にリンクのタップを検知することで誤検知へ対処する様子を示す．提案手法は，図 3 の (4) の遷移時に (1) の遷移時刻からの経過時間を算出する．ここでは，リンクのタップによる誤検知へ対処するため，直近 3 回の切り替わりのいずれか（図 3 の (2)〜(4)）をリンクのタップによる遷移と判別している場合，(4) の遷移を悪性 Web サイトへの遷移と判定しないこととする．直近 1 回ではなく 3 回としている理由は，タップ時に上記のイベントが発生しないリンクがいくつか存在するためである．

なお，悪性 Web サイトへ遷移する際，遷移元サイトから悪性 Web サイトまでリダイレクトが連続して 3 回以上発生することが多い．また，リダイレクト時には “TYPE_VIEW_CLICKED” は発生しないため，直近 3 回の遷移はリンクのタップによる遷移と判別されない．以上より，悪性 Web サイトへの遷移の検知への影響はない．

3.3.2 （対処 2）「戻る」操作を検知する方法

「戻る」ボタンを押下時に特定のイベントが発生する場合，そのイベントを検知することで「戻る」操作を連続で実行した際に発生する誤検知をすべて抑制できると推察

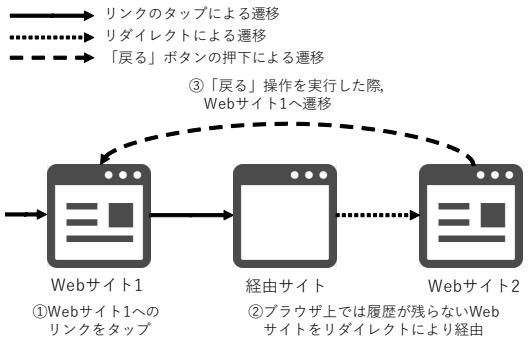

図 4 「戻る」操作を実行時に 2 つ前の Web サイトへ遷移する例

する．しかし，「戻るボタン」の押下時にイベントが発生しない端末（Pixel 3a (Android 10) など）がある．また，Android 10 では，画面の端からのスワイプを「戻るボタン」の押下と同等の操作として設定できる．さらに，この操作時には特定のイベントが発生せず，この操作を検知することはできない．このため，「戻るボタン」の押下を検知することでこの誤検知へ対処することは難しい．

そこで，過去に閲覧した Web サイトの情報を保持して，閲覧した Web サイトへ逆順の遷移（現在閲覧している Web サイトの 1 つ前に閲覧していた Web サイトへの遷移）は，悪性 Web サイトへの遷移と判定しないことで対処する．また，良性 Web サイトでは，**図 4** に示すよう履歴が残らない遷移が発生する場合がある．図 4 では，Web サイト 1 において Web サイト 2 へのリンクをタップした際，履歴が残らない 1 つの Web サイトをリダイレクトにより経由する．このため，Web サイト 2 において「戻るボタン」操作を実行した際，Web サイト 1（2 つ前に閲覧していた Web サイト）へ遷移する．ここで，提案手法は経由した Web サイトの情報を保持しており，これを逆順の遷移と判断しない．以上より，現在閲覧している Web サイトの 1 つ前だけでなく，2 つ前に閲覧していた Web サイトへの遷移も「戻る」操作による遷移と判別する．

3.3.3 （対処 3）その他の操作による遷移を検知する方法

3.2 節で述べたよう良性 Web サイトには，特定の操作により Web サイトが切り替わる事例がある．また，3.3.1 項で述べたようリンクのタップ時にイベントが発生しないリンクがいくつか存在する．そこで，上記 2 つの対処では誤検知を抑制できない Web サイトのドメインのホワイトリストを作成することで，これに対処する．具体的には，ホワイトリストのドメインへの遷移は経過時間に関係なく，悪性 Web サイトへの遷移とは判定しないとする．

ここでは，Alexa Top Sites (Japan)[11] の 1 位から 50 位までの Web サイトを調査して，誤検知を抑制できない Web サイトのドメインのホワイトリストを作成する．ホワイトリストに登録するドメインは，意図しない操作による悪性 Web サイトへの遷移でないものの，URL バーが短い間に連続して切り替わる可能性のある Web サイトのドメ

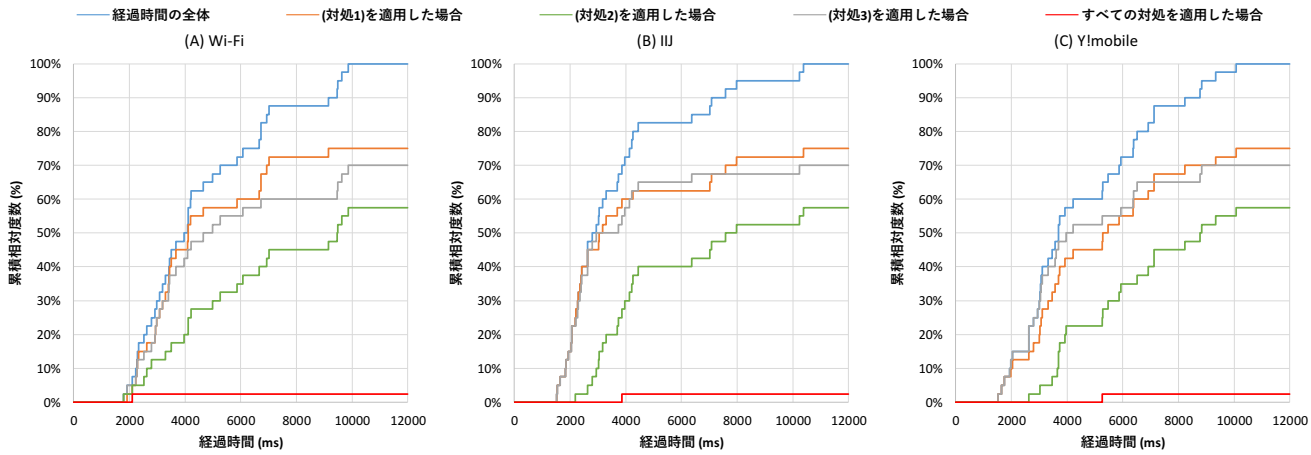

図 5　良性 Web サイトの経過時間とその累積相対度数

表 2　評価環境

	(A) Wi-Fi (岡山大学)	(B) IIJ (docomo)	(C) Y!mobile (Softbank)
OS	Android 10	Android 9.0	Android 7.1.2
CPU	Snapdragon 845, 2.8 GHz	Snapdragon 845, 2.5 GHz	Snapdragon 617, 1.5 GHz
メモリ	4GB	4GB	2GB
Google Chrome	84.0.4147.111	84.0.4147.111	84.0.4147.111

インを対象とする．なお，2020 年 5 月 26 日時点の Alexa Top Sites を用いて，13 のドメインを登録した．また，このホワイトリストは 4 章に後述する実証実験データを用いた評価結果に基づいて，今後拡張していく予定である．

3.4　検知精度の評価

3.4.1　評価内容

ここでは，改善した提案手法が改善前と比較して性能が優れていることを示すため，良性 Web サイト，および悪性 Web サイトを用いて提案手法の検知精度を評価する．これにより，3.3 節で述べた 3 つの対処がどのくらい検知精度に寄与したのかを示す．なお，評価は**表 2** に示す実際の Android の利用を想定した 3 つの環境において実施する．

また，評価にはセンサアプリのサンプルアプリを用いる．このアプリは，WarpDrive の実証実験において参加者のスマートフォンにインストールするセンサアプリ（4.1 節に後述）が収集する情報と同様の情報を収集する．このため，このアプリを提案手法の検証に用いることができる．

3.4.2　評価方法

良性 Web サイトとして，2020 年 5 月 26 日時点での Alexa Top Sites の 1 位から 50 位までの Web サイトを用いる．良性 Web サイトの評価手順を以下に示す．

(1) これらの Web サイトにおいて，リダイレクトが用いられることがある操作（ログイン，ログアウトなど）を実行する．
(2) 各 Web サイトを利用する操作（ショッピングサイトであれば，商品ページを閲覧）を実行する．
(3) (2) の後，「戻る」操作を連続して実行する．
(4) サンプルアプリにより，上記の各操作のログを収集して，検知結果，URL バーの切り替わり時刻を記録する．また，各操作の経過時間を算出する．

また，悪性 Web サイトとして，文献 [12] で提案している手法により収集した URL のうち，2020 年 7 月 7 日時点で悪性 Web サイトへの遷移が発生する 33 件の遷移元サイトを用いる．悪性 Web サイトの評価手順を以下に示す．

(1) これらの遷移元サイトにおいて，悪性 Web サイトへの遷移を発生させる．
(2) サンプルアプリにより，各遷移のログを収集して，検知結果，URL バーの切り替わり時刻を記録する．また，各操作の経過時間を算出する．

3.4.3　評価結果

まず，3.4.2 項で算出した良性 Web サイトにおける経過時間とその経過時間の累積相対度数を表すグラフを**図 5** に示す．図 5 には，Wi-Fi，IIJ，および Y!mobile の各環境のグラフを記載しており，横軸が経過時間，縦軸が経過時間の累積相対度数を示している．また，青線が全体の経過時間を示しており，橙線がリンクのタップを検知する方法（対処 1）を適用した場合，緑線が「戻る」操作を検知する方法（対処 2）を適用した場合，灰色線がホワイトリスト（対処 3）を適用した場合，および赤線がすべての対処を適用した場合の誤検知率を示している．図 5 より，改善後の提案手法は（閾値 2）をこれまでの「4,000ms」から十分に長い値である「10,000ms」へ変更した場合でも，すべての環境にて誤検知率は 2.5%に抑制できることがわかる．これより，3.3 節で述べたすべての対処を適用することで（閾値 2）を長くした場合でも，誤検知を抑制できる．

また，悪性 Web サイトにおける経過時間とその経過時間の累積相対度数を表すグラフを**図 6** に示す．図 6 は横軸が経過時間，縦軸が経過時間の累積相対度数を示している．

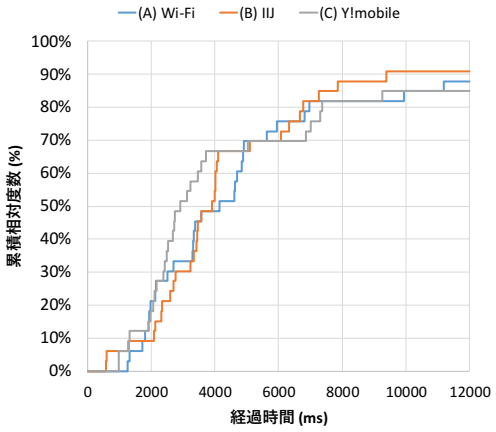

図 6 悪性 Web サイトの経過時間とその累積相対度数

また，青線が Wi-Fi 環境，橙線が IIJ 環境，および灰色線が Y!mobile 環境の結果を示している．図 6 より，(閾値 2) がこれまでの「4,000ms」の場合，検知率は Wi-Fi 環境にて 48.4%，IIJ 環境にて 51.5%，Y!mobile 環境にて 66.7% である．これに対して，(閾値 2) を十分に長い値である「10,000ms」とした場合，検知率は Wi-Fi 環境にて 84.9%，IIJ 環境にて 90.9%，Y!mobile 環境にて 84.9%となる．なお，ここでは，遷移元サイトから悪性 Web サイトまでのリダイレクト数が 2 回以下であるため，遷移する際の経過時間が算出されない事例を検知できていない．

以上より，3 つの対処によって，提案手法の誤検知率を抑制しながら (閾値 2) を十分に長い値に設定でき，これにより悪性 Web サイトの検知率を向上できることを示した．

4. Web 媒介型攻撃観測システムによる収集データを用いた提案手法の評価

4.1 Web 媒介型攻撃観測システムについて

Drive-by Download 攻撃などの Web に関連する攻撃に対して，実証実験を行う Web 媒介型攻撃対策技術の実用化に向けた研究開発 (WarpDrive) がある [8]．WarpDrive では，近年 Web 媒介型攻撃がスマートフォンに拡大していることから，スマートフォンを対象にしたユーザ参加型の Web 媒介型攻撃観測システムを提案している [9]．このシステムは，参加者のスマートフォンにインストールするセンサアプリとデータを収集して分析するデータ収集・分析サーバから構成されている．センサアプリは，Web アクセス履歴，アプリ表示履歴，および端末情報などを収集して，これらの情報 (以降，実証実験データ) を分析に利用する．

センサアプリには，悪性 Web サイトへの遷移を検知することを目的として，3.3 節で述べた 3 つの対処を施した提案手法を実装しており，悪性 Web サイトへの遷移を検知した際，**図 7** に示すようアニメキャラクターが警告する．現時点では誤検知を考慮して，フォアグラウンドに警告を表示するのみでユーザ操作には影響を与えない実装となっている．また，提案手法の閾値は 3.4.3 項で良性 Web サイトの誤検知率が低く，悪性 Web サイトの検知率が高い結果を示した「10,000ms」としている．

©士郎正宗・Production I.G/講談社・攻殻機動隊製作委員会

図 7 センサアプリの悪性 Web サイトへの遷移を検知した際の警告表示の様子

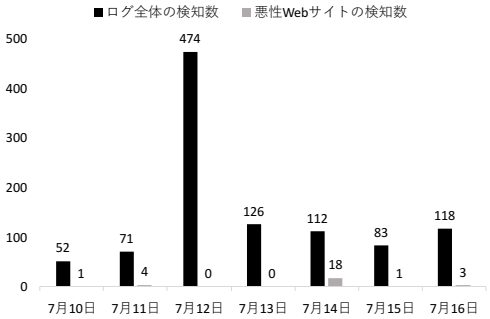

図 8 実証実験データによる提案手法の検知精度

なお，センサアプリは，Google Play にて「タチコマ・セキュリティ・エージェント・モバイル」として配布されている．また，センサアプリは，収集データの中から個人情報および個人に紐付く情報を機械的に削除して収集する [9]．

4.2 実証実験データの集計および評価

提案手法の有用性や今後の課題を明確にすることを目的として，実証実験データを用いた提案手法の検知精度を評価する．提案手法は，7 月 10 日に配布されたアップデートにて更新されたセンサアプリに実装しており，提案手法を実装したセンサアプリにより収集した実証実験データには，Web アクセスが悪性 Web サイトへの遷移と判定されたか否かを示す情報が含まれる．このため，評価対象のデータは，提案手法が実装されたセンサアプリにより収集されたデータを対象とする．ここでは，2020 年 7 月 10 日から 7 月 16 日の期間に収集されたデータを対象とする．

4.3 実証実験データによる検知精度

評価対象のログについて，提案手法によるログ全体の検知数，およびそのうち悪性 Web サイトへの遷移の検知数を表すグラフを**図 8** に示す．図 8 より，全体の検知数のうち，悪性 Web サイトへの遷移の検知数が極めて少なく，多くの誤検知が発生していることがわかる．このため，実証実験データによる評価に基づいてホワイトリストの拡張や閾値の再検討を実施する必要がある．

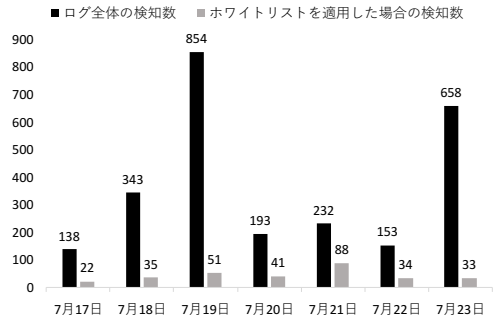

図 9 ホワイトリストを適用した場合の検知数の変化

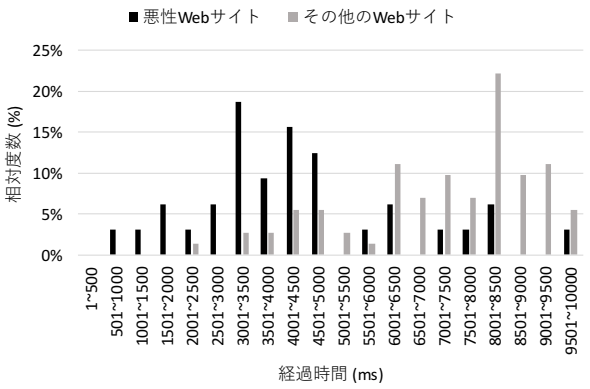

図 10 悪性 Web サイトとその他の Web サイトへ遷移する際の経過時間

4.4 提案手法の再検討

現状では，多くの誤検知が発生している問題点への 1 つの対処としてホワイトリストを拡張する方法がある．実証実験データを確認した限りでは，同様の Web サイトにて多くの誤検知が発生している事例がいくつかある．このため，誤検知数が多い Web サイトのドメインをホワイトリストに登録することで誤検知数を大幅に減少できると推察する．そこで，評価対象のログの中で誤検知数が 3 以上のドメインをホワイトリストへ追加することを検討する．

2020 年 7 月 17 日から 7 月 23 日の期間に収集されたログのうち，提案手法によるログ全体の検知数，および上記のホワイトリストを適用したと仮定したログ全体の検知数を表すグラフを**図 9** に示す．図 9 より，拡張したホワイトリストを適用した場合，誤検知数を大幅に減少できる．

また，提案手法の誤検知数をさらに減少するため，提案手法の閾値を再検討する．**図 10** に提案手法により検知したログのうち，悪性 Web サイトへの遷移であると正しく検知したログ，およびその他のログの経過時間の相対度数を表すグラフを示す．図 10 より，悪性 Web サイトへ遷移する際の経過時間は 75%が 5,000ms 以下であり，その他の経過時間は，78%が 6,001ms 以上である．

さらに，図 10 の検知ログのみを利用して，提案手法の経過時間の閾値と FPR， FNR の関係を調査した結果を**図 11** に示す．図 11 のデータラベルは提案手法の経過時

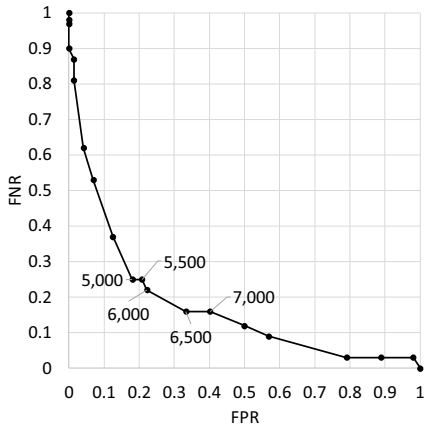

図 11 提案手法により悪性 Web サイトへの遷移であると判定したログの経過時間の閾値と FPR, FNR の関係性

表 3 検討内容を適用したと仮定の下での検証結果

トータルログ数	検知したログ数	検知率	誤検知率
218,486	136	0.0622%	0.0188%

間の閾値を表しており，横軸はその閾値の FPR（誤検知率），縦軸はその閾値の FNR（見逃し率）を示している．図 11 より，FPR と FNR の両者が 0 に近い閾値（5,000ms や 6,000ms）では，誤検知率を低い値に抑制しながら，悪性 Web サイトの検知率が高い結果が期待できる．以上より，経過時間の閾値を 6,000ms に変更することで，提案手法の検知精度をより向上できる可能性がある．

ここで，上記のホワイトリストを適用，および閾値を「6,000ms」へ変更したという仮定の下で，2020 年 7 月 17 日から 7 月 23 日の期間に収集されたログを検証した場合，**表 3** に示す結果が得られる．表 3 より，実際は設定した閾値以上で 3 回遷移する Web アクセスが多く，トータルログ数を考慮した場合は検知率，および誤検知率は非常に低くなる．このことから，提案手法は，実利用のおける誤検知数は非常に少なく，悪性 Web サイトに対して閲覧前に危険性を警告できるため，有用性がある．

5. 関連研究

利用者を悪意のある Web サイトへ誘導する際，リダイレクトが用いられる場合がある．このリダイレクトに着目した先行研究が存在する [1], [5].

文献 [1] では，Drive-by Download 攻撃で発生する多段のリダイレクト情報を高対話型ハニークライアントによって自動的に収集して，リダイレクト情報の構造的類似性に基づいた検知手法を提案している．文献 [5] では，悪性 Web サイトへ遷移する際の多段のリダイレクトのフローを表すグラフを大量に作成して，このグラフの特徴に基づいた検知手法を提案している．しかし，上述の文献はリダイレクトにより複数の Web サイトを経由する特徴に着目しているものの，Android に着目していない．

また，モバイルのアプリ内広告によるクリック詐欺の被害が報告されている [13]．クリック詐欺は，自動で広告をクリックすることでアプリ開発者が利益を得ることを目的としている．これが悪意のある広告に対して実施される際，リダイレクトにより悪意のある Web サイトへ誘導される可能性があり [14]，この特徴は我々が調査対象としている利用者の意図しない Web サイトへの遷移に類似している．

文献 [13] では，ディープラーニングベースのモデルを提案しているものの，これはクリック詐欺検出を目的としており，利用者の意図しない Web サイトへの遷移の検知には適用できない．文献 [14] では，リダイレクトに着目しており，悪意のある Web サイトへ遷移する際はリダイレクトチェーンがより長いことを明らかにしているものの，対策については検討されていない．

さらに，Web サイトの全体を覆う透明，または半透明の広告を用いる手段などにより，強制的に広告クリックを引き起こすことで悪意のある Web サイトへ誘導する被害が報告されている [15]．文献 [15] は，Android に着目していないものの，悪性 Web サイトへ誘導する攻撃に類似する攻撃を体系的に調査している．また，対策として，Web サイトが攻撃に関連する URL を含む場合，その URL と警告メッセージを表示することを検討している．

6. おわりに

文献 [6] で提案したアクセシビリティサービスを用いた URL バーの切り替わり間隔に着目した利用者の意図しない Web サイトへの遷移の検知手法について，悪性 Web サイトの見逃し率が高いという問題点へ対処するため，3 つの改善手法を提案した．具体的には，リンクのタップの検知，「戻る」操作の検知，およびホワイトリストの利用により，良性 Web サイトへの遷移と悪性 Web サイトへの遷移を判別することで上記の問題点へ対処した．また，改善した提案手法について，良性 Web サイトと悪性 Web サイトの検知精度を示した．これにより，誤検知率を抑制しながら悪性 Web サイトの検知率を向上できることを示した．

さらに，Web 媒介型攻撃観測システムにより収集した実証実験データを用いて提案手法の評価を実施した．この評価により，良性 Web サイトにおける短い間に連続する Web サイトの切り替わりを検知してしまう課題を発見し，この改善手法について提案し，実証実験データに基づくシミュレーションにより，検知精度を向上できることを示した．

今後の課題として，実証実験データの評価結果に基づいてホワイトリストの拡張，および再検討した閾値を実装したセンサアプリ[*1]で取得した実証実験結果の評価がある．

謝辞　本研究成果は，国立研究開発法人情報通信研究機構 (NICT) の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」により得られたものです．また，評価にご協力いただいた岡山大学大学院自然科学研究科の横山綾氏，石原聖氏，利穂虹希氏に深く感謝を申し上げます．

[*1] 4.4 節の検討に基づき，改善した提案手法は，タチコマ・セキュリティ・エージェント・モバイルに搭載されており，こちらから利用可能．（https://warpdrive-project.jp/mobile-app/）

参考文献

[1] Shibahara, T., Yagi, T., Akiyama, M., et al.: POSTER: Detecting Malicious Web Pages Based on Structural Similarity of Redirection Chains, *Proc. 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS'15)*, pp.1671–1673, (2015).

[2] Meridith Levinson: Mobile Malware: Beware Drive-by Downloads on Your Smartphone, CIO, available from ⟨https://www.cio.com/article/2397969/mobile-malware--beware-drive-by-downloads-on-your-smartphone.html⟩ (accessed 2020–08–05).

[3] Aravindhan, R., Shanmugalakshmi, R., Ramya, K., et al.: Certain investigation on web application security: Phishing detection and phishing target discovery, *Proc. 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, (2016).

[4] Trishita, T., Ari, T.: Alternative (Ab)Uses for HTTP Alternative Services, *Proc. 13th USENIX Conference on Offensive Technologies (WOOT'19)*, (2019).

[5] Stringhini, G. et al.: Shady Paths: Leveraging Surfing Crowds to Detect Malicious Web Pages, *Proc. 2013 ACM SIGSAC Conference on Computer; Communications Security (CCS'13)*, pp.133–144, (2013).

[6] 折戸凜太郎，佐藤将也，山内利宏：Android における URL バーの切り替わり間隔に着目した利用者の意図しない Web サイトへの遷移の検知手法，コンピュータセキュリティシンポジウム 2019 論文集，pp.1017–1024，(2019)．

[7] 折戸凜太郎，石原聖，佐藤将也，梅本俊，中嶋淳，山内利宏：Android における URL バーの切り替わり間隔に着目した利用者の意図しない Web サイトへの遷移の検知手法の評価，2020 年暗号と情報セキュリティシンポジウム（SCIS2020）論文集，電子媒体，(2020)．

[8] WarpDrive, 入手先 ⟨https://warpdrive-project.jp/⟩ (参照 2020–08–05)．

[9] 山田明，佐野絢音，窪田歩ほか：スマートフォンにおける Web 媒介型サイバー攻撃の観測機構：設計と実装，2020 年暗号と情報セキュリティシンポジウム（SCIS2020）論文集，電子媒体，(2020)．

[10] Imamura, Y., Orito, R., Chaikaew, K., et al.: Threat Analysis of Fake Virus Alerts Using WebView Monitor, *Proc. 2019 Seventh International Symposium on Computing and Networking (CANDAR)*, pp.28–36 (2019).

[11] Alexa：Top Sites in Japan, 入手先 ⟨https://www.alexa.com/topsites/countries/JP⟩ (参照 2020–08–05)．

[12] 石原聖，折戸凜太郎，佐藤将也，山内利宏：モバイル向け悪性 Web サイトの探索によるブラックリスト構築手法，コンピュータセキュリティシンポジウム 2019（CSS2019）論文集，pp.1025–1032，(2019)．

[13] Thejas, G. S. et al.: Deep Learning-Based Model to Fight Against Ad Click Fraud, *Proc. 2019 ACM Southeast Conference (ACM SE'19)*, pp.176–181, (2019).

[14] Gong, C., Wei, M., John, C.: Revisiting Mobile Advertising Threats with MAdLife, *Proc. World Wide Web Conference (WWW'19)*, pp.207–217, (2019).

[15] Mingxue, Z., Wei, M., Sangho, L., et al.: All Your Clicks Belong to Me: Investigating Click Interception on the Web, *Proc. 28th USENIX Conference on Security Symposium (SEC'19)*, pp.941–957, (2019).