

攻撃者の属性情報を用いた不正アクセスの分析

邦本 理夫^{1,2,a)} 大久保 隆夫²

概要：近年、インターネットバンキングやクレジットカード等の不正利用による被害が大きな問題となっている。不正利用を行う攻撃者は、フィッシングメールやマルウェア等で被害者の認証情報を詐取して不正行為を行っており、攻撃手法の巧妙化と被害の拡大は深刻な社会問題となっている。こうした不正行為に対しては、利用者側での対策が有効であり、金融機関は利用者向けに注意喚起を継続的に行ったり、無償でフィッシング対策ソフトを提供するなどの対策を行っている。しかしすべての利用者に対策ソフトの導入を強制するのは利便性の観点から困難であるなど、対策を徹底することは難しく、継続して被害が発生している。このように利用者側での対策の徹底が困難である現状を踏まえ、本稿ではサーバ側で実施可能な不正検知の手法について検討を行った。不正送金を行う攻撃者の端末情報や IP アドレスなどの属性情報の特徴について、実際の不正アクセスのログを元に分析を行い、攻撃者と正規利用者の属性情報の差異を調査した。また調査結果に基づいて、属性情報を元に攻撃者のアクセスを検知する手法について考察した。

キーワード：不正検知, Browser Fingerprint, ネットワーク情報

Analysis of Fraudulent Access Using Attackers' Attribute Information

Abstract: Fraudulent access against internet banking, credit card and e-commerce has been serious problem. Illicit use of stolen credentials due to malware infection and phishing sites are reported continuously, and these attack methods are being more sophisticated. Client-side countermeasures are effective against these frauds and many financial organizations provide anti-phishing software, but it is usually difficult for the companies to force their end-users install additional software because it may cause trouble and decrease usability. Regarding these issues we are researching the effective fraud detection method using server-side log information. In this paper, we show the analysis result of the attackers' attribute data from the logs of actual services and analyse the difference of the attribute information between attackers and legitimate users.

Keywords: Fraud Detection, Browser Fingerprint, Network Information

1. はじめに

近年、インターネットバンキングやクレジットカード、EC サイト等に対する不正アクセスが大きな問題となっている。警察庁の統計では、インターネットバンキング等への不正アクセスによる被害件数および被害額は 2015 年をピークとして 2018 年までは減少傾向にあったが [1], 2019 年 9 月以降に被害が急増し、2019 年 11 月には単月で 7 億

7600 万円という過去最悪の被害が発生した (図 1)。この被害急増に対し、警察庁および全国銀行協会が連携して不正送金被害の防止に係る啓発を実施している [2], [3]。また日本クレジット協会の統計では、クレジットカードの番号盗用による不正利用が近年急激に増加しており、2018 年には 187 億円余りの被害が発生している [4]。

こうした不正行為を行う攻撃者が、インターネットバンキングのアカウントやクレジットカード番号等の情報を取得するための手段として、フィッシングサイトやマルウェア等が用いられている。フィッシング対策協議会の統計を図 2 および図 3 に示す。この統計によると、フィッシングの報告件数およびフィッシングサイトの URL 数がいずれも増加傾向にある。

¹ 株式会社セキュアブレイン
SecureBrain Corporation, Chiyoda, Tokyo 102-0094, Japan
² 情報セキュリティ大学院大学
Institute of Information Security, Yokohama, Kanagawa
221-0835, Japan
^{a)} michio_kunimoto@securebrain.co.jp

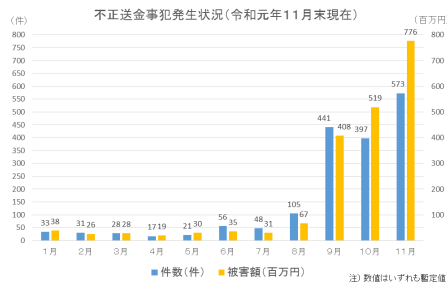


図 1 不正送金発生状況 (出典: [2])

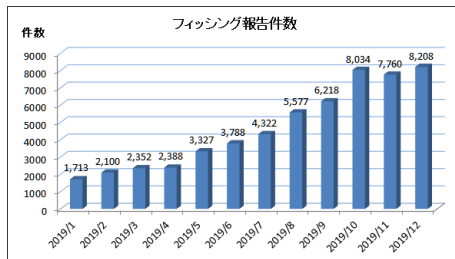


図 2 フィッシング検知件数の統計 (出典: [5])

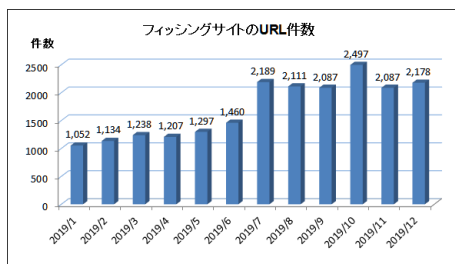


図 3 フィッシング URL 数の統計 (出典: [5])

フィッシング対策では、原理的にフィッシングサイトの作成やフィッシングメールの配信自体を防止することは困難なため、クライアント側にフィッシング対策のソフトウェアをインストールする等、利用者がフィッシングサイトへアクセスすることを防止する手段が必要となるが、セキュリティ対策を行わない利用者は一定数存在する。インターネットバンキング等のホームページでは、無償でフィッシング対策ソフト等を提供し、利用者に対してセキュリティ対策を呼びかけているが、対策ソフトのインストールを強制することは、利用者の利便性を損ねることになり困難である。

こうした背景から、筆者はサーバ側で不正アクセスを検知する仕組みについて研究を行っている。フィッシング等を行う攻撃者は、盗んだ認証情報を用いて対象のシステムにログインし不正行為を行うことから、攻撃者のアクセスログもシステム上に残っている。そのため、ログとして収集できる情報から正規利用者と攻撃者を識別することができれば、クライアント側にソフトウェアをインストールすることなく効果的な不正対策を行うことができる。

ウェブシステムがログとして収集できるクライアントの情報には以下のようなものがある。

ネットワーク情報

ネットワーク情報とは、HTTP(S)等の通信プロトコルの中で取得できる情報であり、HTTPヘッダに含まれる情報(IPアドレス、UserAgent等)やTLS通信の情報(TLS Fingerprint)などを含む。

Browser Fingerprint

Browser Fingerprintとは、ユーザの利用するウェブブラウザから取得でき、個別端末を識別するのに利用可能な情報であり、ブラウザの種別や設定のほか、端末のOSやハードウェアなどの情報も含まれる。

利用者の振る舞い

利用者の振る舞いは、時刻情報やアクセス元の地域、ウェブシステム上での画面遷移などを指す。振る舞いによる不正検知の一例として、同一の顧客IDを使用したアクセスが短時間に極端に離れた地域(日本と外国など)から発生した場合などがある。

本稿では、実際に筆者が運用している不正検知システムのログからこれらの情報を収集・分析し、不正アクセスの特徴および正規利用者との差異について分析を行った結果について示す。またこの結果を踏まえた今後の研究予定について述べる。

2. 関連研究

本章では関連する先行研究と本研究との差異について述べる。

2.1 Browser Fingerprint

Browser Fingerprintを用いて端末を特定する研究は、2009年のMayerの研究[6]を初めとして複数行われている。Mayerは実験環境でブラウザのnavigator, screen, navigator.plugins, navigator.mimeTypesオブジェクトを収集し、1328件のクライアントのうち1278件(96.23%)を一意的に識別した。

2010年にはEckersleyがソーシャルメディアやウェブサイトを使用して2週間の実験を行い、470,161件のFingerprintを収集して分析を行った[7]。EckersleyはHTTPヘッダ、JavaScriptおよびプラグインの情報を使用して83.6%の一意性を確認し、FlashもしくはJavaが有効な場合には識別率が94.2%まで上がると主張した。この研究で”Browser Fingerprinting”という用語が提示され、また大規模なデータでその有効性が示された。

Eckersleyの研究の後、Browser Fingerprintingに新しい情報を追加する様々な研究が行われている。以下に代表的

な研究を示す。

- Canvas

Canvas API はグラフィックス描画および操作のための API であり、この機能を使用することでブラウザ上で直接図形の描画やレンダリングを行うことができる。2012 年に Mowery と Shacham が、Canvas API を利用した Fingerprint に関する研究を行った [8]。Mowery らは OS、ブラウザバージョン、グラフィックカード、インストールされているフォントなどの要素が描画に関連していることを示し、300 のサンプルから 50 の異なるパターンを示した。その後 Acer らが 2014 年に大規模な研究を行い、その結果を *fingerprintjs* として GitHub に公開した [9]。

- WebGL

Khronos Group が、ブラウザ上でインタラクティブに 3D オブジェクトをレンダリング可能な WebGL API を公開した。Mowery らは Canvas と同様に WebGL についても実験を行い、270 のサンプルから 50 の異なるパターンを示した。その後 2017 年に Cao らが WebGL に強く依存した Browser Fingerprinting 手法を提案し、1903 のサンプルに対して 99% 以上の識別率を示した [10]。

- Browser Extension

近年のブラウザはブラウザ拡張 (Browser Extension) によるカスタマイズ機能を有し、パスワードマネージャや広告ブロッカーなどの拡張は一般的に広く利用されている。Sjoesten らは、利用者を特定の URL にアクセスさせることでブラウザ拡張がインストールされているかどうかを検知する研究を行った [11]。しかしすべてのブラウザ拡張が検知できるわけではなく、Chrome 拡張 43,429 件中 12,154 件、Firefox 拡張 14,896 件中 1,003 件が検出可能であった。

ブラウザ拡張に関する第 2 の研究として、Starov と Niki-forakis の研究がある [12]。Starov らはブラウザ拡張による DOM ツリーの変更を検出する手法を提案し、854 ユーザ、1,656 のブラウザ拡張を対象とした実験において、14.10% のユーザを一意に識別した。

第 3 の研究として、Sanchez-Rola らはブラウザ拡張を検出するためのタイミングサイドチャネル攻撃の手法を提案した [13]。著者らの研究では、存在するブラウザ拡張と存在しないブラウザ拡張に対するリソースの呼出時間の差異を利用して検出が可能であるとしており、204 ユーザに対する実験で 56.86% のユーザを一意に識別した。

ブラウザ拡張に関しては、近年 Gulyas らが大規模な実証実験を行った [14]。16,393 人の参加者に対して Sjoesten らの手法を適用して実験を行い、7,643 人の Chrome ユーザについて 39.29% を一意に識別した。この実験で著者らは 16,743 のブラウザ拡張を対象としたが、対象を特徴の出

やすい 485 のブラウザ拡張に絞っても同等の結果が得られることを合わせて示した。

これらの Browser Fingerprint に関する研究は、いずれもアクセス元の端末を一意に識別することを目的としている。Browser Fingerprint による端末特定をフィッシング対策等の不正検知に応用する場合、攻撃者の端末を特定するためには、一度攻撃者からのアクセスを受け、その Fingerprint が攻撃者のものであると記録しておく必要がある。実際の攻撃者は端末環境を頻繁に変えてくる場合もあり、一度攻撃を受けてからでないと攻撃者のアクセスが識別できない仕組みには実用上の課題が残る。そのため本研究では、攻撃者の端末情報だけではなく、より広い範囲の属性情報を分析して攻撃者の識別を行うことを目的として分析を行っている。

2.2 不正検知

Browser Fingerprint を不正検知に応用した研究として、Bursztein らが 2016 年に Picasso を提案した [15]。Picasso は Canvas 要素を使用して OS およびブラウザの特定を行う仕組みであり、複数回の異なる図形描画を行うことで精度を向上させている。実環境での実験においては、5200 万件のアクセスに対して 100% の精度でブラウザ、OS の組合せが識別可能であった。著者らはこの仕組みを使用して、エミュレータやスクリプトによる環境を偽装した攻撃を検知可能であるとしている。Picasso は端末環境の特定による UserAgent の偽装を検知することが主な機能であり、スクリプト等の検知には効果があると考えられるが、本研究の目的であるフィッシング等を使用する攻撃者の検知とは対象が異なる。

また 2016 年に Freeman らは、不審なログインを判別して追加認証を行うフレームワークを提案し、実データでのプロトタイプ評価を行った。この研究では主な評価要素として IP アドレスおよび UserAgent を使用している。[16]。本研究では IP アドレスや UserAgent のみではなく Browser Fingerprint の各要素も含めて不正判定を行っている点が異なっている。また銀行向けの不正送金検知に特化したシステムとして、Michele らが BANKSEALER や FRAUDBUSTER を提案した [17], [18]。これらはインターネットバンキングシステム上での利用者の消費行動のパターンをプロファイリングすることで異常を検知するシステムである。本研究は特定のシステム上の振る舞いではなく攻撃者の属性情報を元に検知を行っている点が異なる。

3. 実データの分析

筆者は主に Browser Fingerprint およびネットワーク情報から攻撃者と正規利用者の環境の差異を特定できないかと考え、実際のサービスのログを対象に分析を行った。分

析対象のログは筆者が業務で開発・提供している不正検知サービスのログであり、このサービスでは Cookie 等による一意の識別子を用いたブラックリスト判定を行っている。

3.1 対象データ

今回分析対象としたデータの期間および件数について表 1 に示す。なお、対象のシステムには外部サービスの API からのアクセスも行われており、今回の分析は API からのアクセスを除外したデータに対して実施した。ここで攻撃者判定数とは、対象システムの運用者が不正利用と判定した端末からの総アクセス件数を示す。端末の判定には Cookie 等に埋め込んだ一意の識別子を使用している。なお攻撃者判定数は、実際に不正が行われたアクセスの他に、攻撃が未遂に終わったアクセスも含んでおり、また不正検知サービスの仕様上、同一の攻撃者のアクセスを複数回検知することもあるため、実際の被害件数とは等しくない。

表 1 分析対象データ

期間	総件数	分析対象件数	攻撃者判定数
2019/1～12	171,631,789	93,311,194	1,725

3.2 ログに含まれる主なパラメータ

分析対象のログに含まれる主なパラメータを表 2 に示す。

表 2 ログに含まれる主なパラメータ

パラメータ	説明
IPAddress	IP アドレス
UserAgent	ユーザエージェント
AcceptLanguage	言語
TimezoneOffset	タイムゾーン
ScreenWidth	画面の幅
ScreenHeight	画面の高さ
Plugins	インストール済みプラグイン
Fonts	インストール済みフォント
DefaultCharSet	デフォルトの文字コード
JavaEnabled	Java が有効かどうか
WebGLRenderer	WebGL を扱うレンダラーの種別
HardwareConcurrency	論理 CPU 数

4. 分析結果

4.1 攻撃者アクセスの統計

2019 年の攻撃者アクセス数を月毎に集計した結果を図 4 に示す。各月で攻撃者のアクセス数にばらつきがあり、2 月～3 月、5 月～8 月、12 月に攻撃が増加している。攻撃が増加したそれぞれの月について攻撃者の属性情報の特徴を分析したところ、攻撃者のアクセス元環境が大きく 4 つのグループに分けられ、それぞれ異なる特徴があることが分かった。以下に各グループの特徴的なパラメータについ

て述べる。

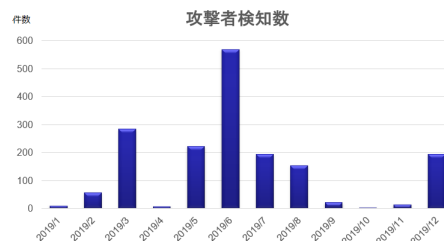


図 4 攻撃者アクセス数

4.2 複数コア GPU からのアクセス

2019 年 3 月の攻撃者アクセスは、複数コア GPU の端末からのアクセスが多いことが分かった。対象期間の攻撃者アクセスを分析した結果、以下の特徴を持つアクセスが全体の過半数を占めた。攻撃者アクセスに含まれるこれらのパラメータと検知件数を表 3 に示す。

- HardwareConcurrency の値が 16 や 20 など一般利用の PC より大きい
- WebGLRenderer が特定の値 (NVIDIA GeForce) を持つ
- 言語設定が中国語

4.3 仮想マシンからのアクセス

2019 年 5 月～6 月の攻撃者アクセスは、仮想マシンからのアクセスが多いことが分かった。仮想マシン環境では、WebGLRenderer がソフトウェアベースのレンダラ名となり、また VMWare を使用している場合は“VMWare”の文字列が含まれるという特徴がある。攻撃者アクセスに含まれる WebGLRenderer の値を表 4 に、また実際に VMWare および VirtualBox を使用して仮想環境を構築し、取得できる WebGLRenderer パラメータの値を確認した結果を表 5 および表 6 に示す。2019 年 5 月～6 月にかけては、過半数の攻撃者が仮想マシンを使用していると考えられ、また一定の割合の攻撃者が Windows Update を行っていない仮想環境からアクセスを行っていることが確認された。

4.4 国外 IP アドレス・クラウドプロバイダからのアクセス

2019 年 7 月～8 月の攻撃者アクセスは、他の期間と比較して国外の IP アドレスからのアクセスが多いことが分かった。アクセス元は大半が中国となっていた。国外 IP からの攻撃者アクセス数を図 5 に示す。

また日本国内のクラウドプロバイダからのアクセスもこの期間に増加していた。特に国内のクラウドプロバイダ A 社の IP アドレスからの攻撃者アクセス数は、2019 年 5 月

表 3 2019 年 3 月の攻撃者アクセスの属性情報 (上位 10 件)

WebGLRenderer	HardwareConcurrency	言語	件数
ANGLE (NVIDIA GeForce GTX 750 Ti Direct3D11 vs_5.0 ps_5.0)	20	zh-CN	108
ANGLE (NVIDIA GeForce GTX 750 Ti Direct3D11 vs_5.0 ps_5.0)	16	zh-CN	64
ANGLE (NVIDIA GeForce GTX 750 Ti Direct3D11 vs_5.0 ps_5.0)	16	ja-JP	18
ANGLE (Intel(R) HD Graphics 5500 Direct3D11 vs_5.0 ps_5.0)	4	zh-CN	16
ANGLE (Intel(R) HD Graphics 4000 Direct3D9Ex vs_3.0 ps_3.0)	4	zh-CN	13
(空文字列)	20	zh-CN	11
(空文字列)	(空文字列)	zh-CN	10
(空文字列)	16	zh-CN	9
ANGLE (Software Adapter Direct3D11 vs_4.1 ps_4.1)	1	ja	7
ANGLE (VMware SVGA 3D Direct3D9Ex vs_3.0 ps_3.0)	1	ja	5

表 4 2019 年 5~6 月の攻撃者の WebGLRenderer (上位 10 件)

値	件数
Google SwiftShader	183
ANGLE (Software Adapter Direct3D11 vs_4.1 ps_4.1)	170
(空文字列)	162
ANGLE (Microsoft Basic Render Driver Direct3D11 vs_5.0 ps_5.0)	96
ANGLE (VMware SVGA 3D Direct3D9Ex vs_3.0 ps_3.0)	85
VMware SVGA 3D	11
ANGLE (AMD 760G (Microsoft Corporation WDDM 1.1) Direct3D9Ex vs_3.0 ps_3.0)	11
ANGLE (Intel(R) HD Graphics 6000 Direct3D9Ex vs_3.0 ps_3.0)	9
ANGLE (Software Adapter Direct3D11 vs_5.0 ps_5.0)	9
unsupported	8

までは 0 件であったものが, 6 月に 17 件, 7 月に 73 件と急増した. その後 8 月に 5 件, 9 月以降は再び 0 件となった.

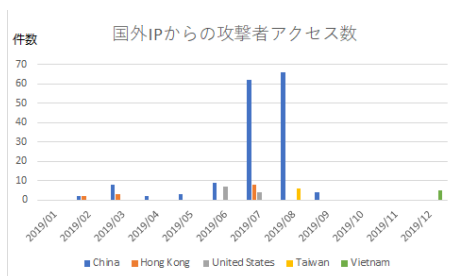


図 5 国外 IP からの攻撃者アクセス数

4.5 iPhone を利用したアクセス

2019 年 12 月の攻撃者アクセスは, iPhone からのアクセスがほぼ全件を占めていた. 言語環境は 8 割以上が日本語で, 次に多いのがベトナム語環境であった. OS のバージョンと言語, 検知件数を表 7 に示す.

5. 正規利用者との比較

正規利用者と攻撃者の属性情報について比較した結果を以下に示す.

5.1 言語

JavaScript で取得できるパラメータ language について, 正規利用者と攻撃者のそれぞれ上位 10 件を表 8 に示す. 攻撃者と正規利用者で, 最もよく使用されているパラメータはいずれも日本語だが, 設定されている値は ja-JP と ja で異なっていた. また攻撃者の約 3 割は中国語環境からアクセスを行っており, 正規利用者の比率に比べて顕著に高い割合であった.

5.2 タイムゾーン

JavaScript で取得できるパラメータ TimezoneOffset について, 正規利用者と攻撃者のそれぞれ上位 10 件を表 9 に示す. 攻撃者と正規利用者で, 最も多い設定はいずれも日本時間 (-540) となっていたが, 攻撃者については約 2 割が中国時間 (-480) となっており, 正規利用者に比べて非常に多い割合となっていた.

5.3 複数コア GPU

2019 年 3 月の攻撃者アクセスで特徴的な属性情報の組合せについて, 正規利用者で同一の属性情報を持つアクセスの有無を確認した結果, 以下の条件を満たす正規利用者からのアクセスは 2019 年を通して存在しないことが確認できた. この属性情報の組み合わせを検知条件とした場合, 誤検知なく攻撃者を検知可能と考えられる. また, HardwareConcurrency が 16 の場合も, 正規利用者と判定

表 5 VMWare 環境での WebGLRenderer

仮想環境	VMWare(R) Workstation 12 Player (12.5.9 build-7535481)				
OS 状態	Windows 7 SP1 (Update なし)		Windows 7 SP1 (Update あり)		
ブラウザ	Chrome 77	Firefox 69	Chrome 77	Firefox 69	IE11
WebGL Renderer	ANGLE (VMware SVGA 3D Direct3D9Ex vs.3.0 ps.3.0)	ANGLE (Software Adapter Direct3D11 vs.4.1 ps.4.1)	ANGLE (VMware SVGA 3D Direct3D11 vs.4.0 ps.4.0)	ANGLE (Software Adapter Direct3D11 vs.5.0 ps.5.0)	VMWare SVGA 3D

表 6 VirtualBox 環境での WebGLRenderer

仮想環境	VirtualBox 6.0.12 r133076				
OS 状態	Windows 7 SP1 (Update なし)		Windows 7 SP1 (Update あり)		
ブラウザ	Chrome 77	Firefox 69	Chrome 77	Firefox 69	IE11
WebGL Renderer	Google SwiftShader	ANGLE (Software Adapter Direct3D11 vs.4.1 ps.4.1)	Google SwiftShader	ANGLE (Software Adapter Direct3D11 vs.5.0 ps.5.0)	unsupported

表 7 2019 年 12 月の攻撃者アクセスの属性情報

OS バージョン	言語	件数
iPhone(iOS 12.4.3)	ja-JP	155
iPhone(iOS 11.4.1)	vi-VN	9
iPhone(iOS 12.4.1)	ja-JP	9
iPhone(iOS 13.1.1)	vi-VN	5
iPhone(iOS 13.1.3)	vi-VN	10
iPhone(iOS 13.1.3)	en-US	3
iPhone(iOS 13.3)	vi-VN	1
Windows10	ja	1

表 8 language の比較

正規利用者		攻撃者	
値	件数	値	件数
ja-JP	55,702,450	ja	800
ja	20,608,093	zh-CN	517
en-US	8,041,078	ja-JP	223
(空文字列)	3,286,688	en-US	61
vi-VN	1,243,401	undefined	51
undefined	587,237	(空文字列)	40
C	459,422	vi-VN	27
ja-jp	362,129	zh-TW	6
zh-CN	333,076		
ko-KR	164,767		

表 9 TimezoneOffset の比較

正規利用者		攻撃者	
値	件数	値	件数
-540	86,901,558	-540	1,304
(空文字列)	3,285,722,108,115	-480	373
-420	354,402	(空文字列)	40
-480	290,606	-420	8
0	78,020		
-120	51,319		
420	48,150		
-60	43,770		
240	35,877		
300	32,508		

6. 考察

ここまでの分析結果を元に、不正検知の効果的な手法について考察する。まず攻撃者が1~2 か月に渡って同一の属性情報を持つ環境からアクセスを行っていることから、攻撃者のアクセスを早期に検知して属性情報を分析することで、その後の被害を防げる可能性があると考えられる。また、複数コア GPU の例では正規利用者で同一の属性情報を持つアクセスが存在しなかったことから、誤検知の少ない検知ルールとして活用できると考えられる。

また、Cookie を使用した識別は精度が高い反面、同一のドメインでしか使用できず、Cookie を削除されると値が変わるなどの制約があるが、本研究で分析を行った属性情報は、攻撃対象のサイトのドメイン等に依存しないため、攻撃対象となっている組織間で情報共有が可能である。そのため早期に攻撃を検知・分析して属性情報を共有することで、全体としての被害を低減させることが出来ると思われる。

一方で、攻撃者の属性情報が変わった場合の対応には課題がある。攻撃者のアクセスを実際に確認してから属性情報をルールとして登録する手法では、新規の環境を使用した攻撃者の初回アクセスを検知することが困難である。攻

されたアクセスは年間で8件のみであり、検知ルールとして有効と考えられる。

- WebGLRenderer が ANGLE (NVIDIA GeForce GTX 750 Ti Direct3D11 vs.5.0 ps.5.0)
- HardwareConcurrency が 20
- language が zh-CN

撃者と正規利用者の環境に統計的な差異は見られたが、そのまま検知ルールとして適用すると誤検知が多発し運用負荷が非常に大きくなる。また 2019 年 12 月の iPhone からのアクセスのように、正規利用者と攻撃者の差が出にくい環境から攻撃が行われた場合、属性情報の分析だけでは対応できないという課題がある。この課題については、画面遷移や時間間隔などの振る舞いや、ID 単位での過去履歴情報との比較など、属性情報以外の要素も組み合わせることで検知精度の向上が期待できると考えており、今後研究を進める予定である。

7. まとめと今後の課題

本稿では、実サービスのログ分析により、攻撃者のアクセスが 1~2 か月に渡って同一の属性情報を持つ環境から継続して行われること、正規利用者と攻撃者で属性情報に差異が見られたことを示した。また特定の属性情報の組合せについては、攻撃者環境固有の値であり、誤検知なく攻撃者を検知可能であることを示した。攻撃者の環境が一定期間同一であることから、早期に攻撃者の特徴を把握することでその後の攻撃者アクセスを検知可能である。また本研究で提示したパラメータについては異なるドメインであっても共有が可能であり、攻撃対象となっている組織間で情報を共有することで、全体としての被害を抑止・低減できる。

本研究の課題として、新規の環境からの攻撃者アクセスの初回検知が困難であること、および正規利用者と攻撃者の属性情報に差異が出にくい場合に検知が困難な点が挙げられる。今後は、攻撃者の振る舞いや個人単位のアクセス履歴なども含めた研究を進め、正規利用者と攻撃者を高精度で識別する手法について提案・実証を進める予定である。

参考文献

- [1] 警察庁：平成 30 年におけるサイバー空間をめぐる脅威の情勢等について (online), 入手先 http://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf (2020.02.17).
- [2] 警察庁：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について (全銀協等と連携した注意喚起) (online), 入手先 <http://www.npa.go.jp/cyber/policy/caution1910.html> (2020.02.17).
- [3] 全国銀行協会：フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の防止に係る啓発の実施について (online), 入手先 <https://www.zenginkyo.or.jp/news/2019/n121901/> (2020.02.17).
- [4] 日本クレジット協会：クレジットカード不正利用被害の発生状況 (online), 入手先 <https://www.j-credit.or.jp/information/statistics/download/toukei.03.g.190930.pdf> (2019.10.28)
- [5] フィッシング対策協議会：2019/12 フィッシング報告状況 (online), 入手先 <https://www.antiphishing.jp/report/monthly/201912.html> (2020.02.17).
- [6] Jonathan R Mayer.: *Any person... a pamphleteer* : *Internet Anonymity in the Age of Web 2.0*, Undergraduate Senior Thesis, Princeton University (2009).
- [7] Peter Eckersley.: *Pixel Perfect: Fingerprinting Canvas in HTML5*, Proceedings of the 10th International Conference on Privacy Enhancing Technologies (PETS' 10). Springer-Verlag, Berlin, Heidelberg, 1-18. (2010).
- [8] Keaton Mowery and Hovav Shacham.: *Handbook of Writing for the Mathematical Sciences*, Proceedings of W2SP 2012, Matt Fredrikson (Ed.). IEEE Computer Society. (2012).
- [9] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz.: *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS ' 14). ACM, New York, NY, USA, 674-689. (2014).
- [10] Yinzhao Cao, Song Li, and Erik Wijmans.: *(Cross-)Browser Fingerprinting via OS and Hardware Level Features*, 24th Annual Network and Distributed System Security Symposium, NDSS. (2017).
- [11] Alexander Sjösten, Steven Van Acker, and Andrei Sabelfeld.: *Discovering Browser Extensions via Web Accessible Resources*, Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy (CODASPY ' 17). ACM, New York, NY, USA, 329-336. (2017).
- [12] Oleksii Starov and Nick Nikiforakis.: *XHOUND: Quantifying the Fingerprintability of Browser Extensions*, 38th IEEE Symposium on Security and Privacy (S&P 2017). San Jose, United States. (2017).
- [13] Iskander Sánchez-Rola, Igor Santos, and Davide Balzarotti.: *Extension Breakdown: Security Analysis of Browsers Extension Resources Control Policies*, 26th USENIX Security Symposium. 679-694. (2017).
- [14] Nataliia Bielova Gábor György Gulyás, Dolière Francis Somé and Claude Castelluccia.: *To Extend or not to Extend: on the Uniqueness of Browser Extensions and Web Logins*, 2018 Workshop on Privacy in the Electronic Society (WPES' 18). (2018).
- [15] Elie Bursztein, Artem Malyshev, Tadek Pietraszek, and Kurt Thomas.: *Picasso: Lightweight Device Class Fingerprinting for Web Clients*, Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM ' 16). ACM, New York, NY, USA, 93-102. (2016).
- [16] David Mandell Freeman, Sakshi Jain, Markus D. Urthum, Battista Biggio, and Giorgio Giacinto.: *Who Are You? A Statistical Approach to Measuring User Authenticity*, 23rd NDSS 2016. San Diego, California, USA. (2016)
- [17] Michele Carminati, Roberto Caron, Federico Maggi, Illeana Epifani, and Stefano Zanero.: *BANKSEALER: A decision support system for online banking fraud analysis and investigation*, Computers and Security, Vol. 53, 175-186. (2015).
- [18] Michele Carminati, Alessandro Baggio, Federico Maggi, Umberto Spagnolini, and Stefano Zanero.: *FraudBuster: Temporal analysis and detection of advanced financial frauds*, Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2018), Vol. 10885 LNCS, 211-233. (2018).