# 属性情報と履歴情報を用いた不正アクセスの分析

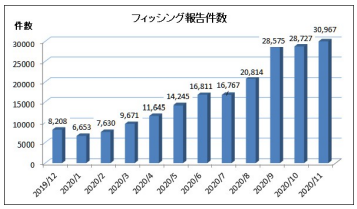
Analysis of Fraudulent Access Using Attribute Information and Access Log History

邦本　理夫・ネットワーク分科会・情報セキュリティ大学院大学

Fraudulent access against internet banking and other services has been serious problem. It is usually difficult for the companies to force their end-users install security software because it may cause trouble and decrease usability. Regarding these issues I am researching the effective fraud detection method using server-side log information. In this paper, I show the analysis result of the attackers' device attribute information and the environmental differences between genuine users and fraudsters based on the access log history, make the rules for detecting the fraudulent access and evaluate the effectiveness. I also discuss the possible changes of the end user environment and the ecosystem of the fraud detection.

## 1. 背景と目的

・成りすましによる不正送金や不正アクセスの被害が近年大きな問題となっている
・対策は利用者のリテラシーに依存する部分もあり完全な対策が困難


**成りすまし犯人は盗んだ認証情報で攻撃対象のウェブシステムにログインする（ログが残る）**
**↓**
**攻撃者のアクセスをウェブシステムのログから識別できないか？**

## 2. ログの分析

### 2-1.分析対象と観点

業務で提供している不正検知サービスの2019年のログを、属性情報と履歴情報の観点で分析

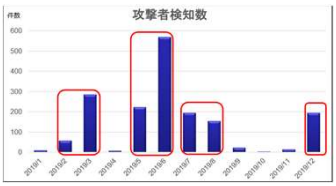
| 期間 | 総件数 | 分析対象件数 | 不正判定数 |
|---|---|---|---|
| 2019/1/1~12/31 | 171,631,789 | 93,311,194 | 1,725 |

【属性情報】
IPアドレス、UserAgent、言語、タイムゾーン等HTTPヘッダやJavaScriptで収集可能な端末情報

【履歴情報】
利用者のIDに紐づく、過去のアクセス時に使用したOSやブラウザの情報

### 2-2.分析結果

攻撃者検知数は月によって増減し、端末環境の特徴が異なる4つのグループが存在した




属性情報および履歴情報を評価した結果、攻撃者のアクセスには下記の特徴が見られた

【属性評価】
-**高性能GPUや仮想マシン利用**などの特徴あり
-履歴評価と比較して高精度で検知可能
（特に類似環境からのアクセスが集中する期間は半数以上の不正アクセスを検知可能）

【履歴評価】
-正規利用者より**低いバージョンのOS、別ブラウザ**を使用する割合が高い
-第一言語が**日本語→中国語**に変化した場合は攻撃者アクセスの可能性が高い
-OSやブラウザのバージョン差異による検知は属性評価と比較すると誤検知が多い

## 3. 検知手法の評価

有効と思われる不正検知条件について、2020年のログを用いて有効性を検証した結果、以下の内容が確認できた

・攻撃者の属性情報の特徴が2019年から2020年で変化しており、属性評価による検知は有効性が低い
・履歴評価は条件によって継続的に有効

| 種別 | 検知条件 | 有効性 |
|---|---|---|
| 属性評価 | 高性能GPUからのアクセス | 低 |
| | 仮想マシンからのアクセス | 低 |
| 履歴評価 | OSのバージョンダウン | 低 |
| | 別ブラウザの利用 | 中 |
| | 第一言語の日本語から中国語への変化 | 高 |

## 4. 考察と今後の課題

・属性評価と履歴評価による不正検知は一長一短（検知精度と有効期間のトレードオフ）
・属性評価による検知は、企業間での情報共有によって、業界全体の被害低減に繋げられる
・正規利用者と類似の端末での攻撃者アクセスの検知は困難なため、振る舞い検知等の検討が必要