第1章　はじめに

インターネットの急速な普及に伴って，情報のアクセスが容易になり，我々の生活が豊かになった一方で，インターネットを悪用したサイバー犯罪が横行している．

サイバー犯罪は，サーバやアプリケーションの脆弱性を利用して，アクセス権限を要する情報を不正に入手したり，サーバに莫大な負荷をかけて，サービスに支障をきたしたりする行為のことである．サイバー犯罪の被害として，顧客の個人情報が流出したり，サービスが長期間，利用できなくなることなどが挙げられる．これらの被害は，サービスを利用する顧客にとっても，サービスを運営する企業にとっても大きな損失となるため，サイバー犯罪の被害を未然に防ぐことはもちろん，被害に遭った際に犯人を特定するための対策を講じることも重要である．

サイバー犯罪の犯人を特定する情報として，多くの場合，IP アドレスが用いられる．サイバー犯罪の被害を受けたサーバのログから，サイバー犯罪に該当するアクセスの IP アドレスを捜査し，インターネットサービスプロバイダに照会を要請することで，犯人の身元を特定することができる．

しかし，技術の進歩により，近年では，IP アドレスのみによる個人の特定は困難になってきている．VPN や Tor を用いることで，インターネットサービスプロバイダから割り振られている本来の IP アドレスを秘匿化してインターネットに接続することができる．また，キャリアグレード NAT の普及により，通常より IP アドレスでの個人の特定が難しくなっていることも事実である．これらの技術についての詳細は，次章で後述する．

そこで，本論文では，サイバー犯罪が発生した際に，IP アドレス以外の方法で犯人を特定する手法について提案する．インターネット利用者が，サーバに送信する情報は複数挙げられるが，その中でも Cookie に着目した特定システムを提案する．Cookie は，Web サーバが Web ブラウザに対して，任意の文字列を記憶させるための仕組みである．サーバから Cookie を保存するように指示されたブラウザは，以降，その Web サイトに対して，記憶した Cookie を送信するようになる．

Cookie を利用することで，サービスのログイン状態を記憶したり，EC サイトにおいて，ショッピングカートの中身を記憶させたりすることができる．一方で，アクセスしてきたユーザに，ユニークな文字列を発行し，Cookie として保存させることで，過去にそのユーザがアクセスしてきたかどうかがわか

るため，個人を特定するために用いられることもある．このように，Cookie はユーザを特定する十分な情報となり得る．

第2章　研究背景

2.1　IP アドレスによる特定の難しさ

発信元の IP アドレスを特定することで，発信者の利用しているインターネットサービスプロバイダやキャリア，地域レベルの位置情報を取得できることが多い．サイバー犯罪が発生した際に，IP アドレスからインターネットサービスプロバイダを特定し，インターネットサービスプロバイダに照会を要請することで犯人を特定することができる．

しかし，技術の進歩により，IP アドレスによる個人の特定は困難であるケースも珍しくない．IP アドレスによる個人の特定が困難となる技術の代表例を以下に示す．

2.1.1　キャリアグレード NAT

キャリアグレード NAT とは，インターネットサービスプロバイダなどが，ネットワークアドレス変換 (NAT) を行う仕組みである．ネットワークアドレス変換とは，同一 LAN 内の各端末に割り振られたプライベート IP アドレスと，インターネットサービスプロバイダから割り振られたグローバル IP アドレスを変換するための仕組みである．IPv4 アドレスの枯渇問題により，インターネットに接続する各端末すべてにグローバル IP アドレスを割り振ることは困難である．そこで，各端末には，グローバル IP アドレスの代わりに，プライベート IP アドレスを割り振り，インターネットに接続する際に，プライベート IP アドレスをグローバル IP アドレスに変換することで，LAN 内の複数の端末を同じグローバル IP アドレスでインターネットに接続させることができる．ネットワークアドレス変換は，各家庭の LAN 内で行われるが，これをインターネットサービスプロバイダ単位で行ったものがキャリアグレード NAT である．

IPv4 アドレスの枯渇問題を解消する手段として，キャリアグレード NAT がしばしば利用されているが，同一のグローバル IP アドレスが，複数のインターネット利用者によって使用されるため，キャリアグレード NAT を使用している場合は，IP アドレスによる個人の特定が困難となる．インターネットサービスプロバイダでは，キャリアグレード NAT を利用した際の IP アドレスの変換テーブルを保持しているが，変換テーブルは，最新の約 2 ヶ月分

しか記録されていないため，保存期間を過ぎると，IP アドレスによる特定ができなくなる．

2.1.2 VPN

2.1.3 Tor

2.2 IP アドレスによる誤認逮捕

2.3 Cookie による個人の特定

IP アドレスによる個人の特定は困難であったり，誤認逮捕を招く可能性があるため，サイバー犯罪において犯人を特定する情報としては，十分とはいえない．そこで，本論文では，Cookie による個人の特定可能性に着目した．

Cookie とは，Web サーバが，Web ブラウザに対して，任意の情報 (文字列) を記憶させるための仕組みである．サーバから Cookie を保存するように指示されたブラウザは，以降，その Web サイトに対して，記憶した Cookie を送信するようになる．

Cookie を利用することで，サービスのログイン状態を記憶したり，EC サイトにおいて，ショッピングカートの中身を記憶させたりすることができる．一方で，アクセスしてきたユーザに，ユニークな文字列を発行し，Cookie として保存させることで，過去にそのユーザがアクセスしてきたかどうかを調べることができる．このように，Cookie はユーザを特定する十分な情報となり得る．

ブラウザがサーバに送信する情報として，使用している言語，ブラウザや OS の種類，バージョンなどが挙げられるが，これらは他のユーザと似たような情報となることが多い上，本来とは異なる情報を送信することも可能である．それに対して，Cookie は，サーバがブラウザに保存するように指示する値であるため，サーバがユニークな値を発行し，発行した値を記録しておくことができる．そのため，他のユーザと区別することができる上，ユーザが，サーバから指示された値とは異なる Cookie を送信しても，詐称したことがわかる．よって，Cookie は，ブラウザがサーバに送信する情報の中でも，個人を特定できる可能性が高いことがわかる．

2.4 SNS による個人の特定

近年，多くのインターネット利用者が SNS を利用している．Twitter 社が公開した”Q2 2017 Letter to Shareholders”によれば，2017 年における Twitter の月間利用者数は 3 億 2800 万人である．また，Facebook 社が公開した”Facebook Q2 2017 Results”によれば，2017 年における Facebook の月間利用者数は約

20 億人である．SNS が発展した現代においては，世界中の人々が，SNS を通じてインターネットに自分の情報を発信しているといえる．

Twitter や Facebook などの SNS には，多くの個人情報が保存されている．そのため，サイバー犯罪の犯人が利用している SNS のアカウントを特定し，SNS を運営する企業に協力を依頼することで，犯人の身元を特定することは十分に可能であると考えられる．

最近の多くの Web サイト，とりわけニュースサイトやブログサイトでは，自身もしくは自社のサイトを読者に広めてもらうために，SNS のシェアボタンを設置していることが多い．SNS のシェアボタンのリソース (画像やスクリプトなど) を読み込むために，ブラウザは SNS のサイトに対してリクエストを送信するが，その際に，ユーザがその SNS にログインした状態であれば，SNS のサーバにセッション情報を含む Cookie を送信しているはずである．

したがって，SNS のシェアボタンを設置したサイトでサイバー犯罪が発生した際，犯人がその SNS にログインした状態であれば，犯人の SNS のアカウントを特定することができる可能性が高いと考えられる．Cookie が個人を特定する情報となり得ることについては前述したが，SNS の Cookie はサイバー犯罪の犯人を特定する上で非常に重要な情報であるといえる．

2.5　犯人の不注意による逮捕事例

SNS による特定は，犯人が SNS にログインしていることが前提である．用心深い犯人であれば，サイバー犯罪を行う前に SNS からログアウトしているか，別のブラウザを使用しているであろう．

しかし，すべてのサイバー犯罪の犯人が，完全に証拠を残さずに犯罪を行うわけではない．実際に，Tor を利用して児童ポルノを投稿した犯人が逮捕された事例がある．Tor を使用することで発信元を隠蔽することができるが，逮捕された犯人は，Tor の利用中に，不注意により通常のブラウザを使用したために発信元を特定されてしまった．このように，犯人の不注意によって逮捕されるケースもある．

SNS において，利用を中断する度にログアウトするユーザは少数であると考えられる．ログインした状態でも通常のインターネットの使用に支障がないためである．よって，SNS にログインした状態で，その SNS のシェアボタンが設置されたサイトにアクセスすることは十分に考えられる．犯人の不注意により SNS のアカウントを特定することは，犯人の特定に大きく寄与するといえる．

第3章　研究方法

3.1　研究目的

第 2 章で述べたように，IP アドレスによる特定は困難である．そのため，サイバー犯罪の犯人を特定する際は，IP アドレスだけでなく，それ以外の情報を元に特定する手法が必要である．本論文では，Cookie が個人を特定できる可能性が高いことに着目した．また，近年において SNS を利用するユーザが多く存在し，ログアウトする機会が少ないことから，サイバー犯罪において，犯人の SNS のアカウントを発見することが，犯人の特定に大きく寄与するのではないかと考えられる．最近では，SNS のシェアボタンを設置する Web サイトが多く見受けられる．SNS のシェアボタンを読み込む際に送信された Cookie を利用することで，サイバー犯罪の犯人を特定する手法を提案することを目的とする．

3.2　提案手法

SNS のシェアボタンを読み込む際に送信された Cookie から，個人をどの程度特定できるか実験するために，本研究では，匿名掲示板サイトと SNS サイトを用意した．

第4章　実装

4.1　匿名掲示板

本研究で使用した匿名掲示板は，インターネット上にフリーソフトウェアとして公開されている，KENT-WEB の LIGHT BOARD である．この掲示板は，アカウント登録が不要で利用できる掲示板サイトである．名前の入力が必須となっているが，実名を入力する必要はなく，投稿毎に別の名前を入力することも可能であるため，匿名掲示板として利用することができる．

本研究では，KENT-WEB の LIGHT BOARD のソースプログラムをダウンロードし，改変したものを，自身のサーバで公開し実験を行った．実験に利用した匿名掲示板サイトを図 4.1 に示す．

図 4.1: 匿名掲示板サイト

掲示板への書込みの際に入力する項目は複数あるが，必須項目は書込みを行った人の名前，書込みのタイトル，本文，画像認証の 4 項目である．画像認証の項目には，入力欄の右側に画像として表示された数字を入力する．これはスパム投稿を防止するためのものである．先述の通り，名前は実名を入

力する必要はないため，個人情報を一切入力せずに投稿できるため，利用者から見ると匿名掲示板のように利用することができる．