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．

第3章　研究方法

3.1　研究目的

　サイバー犯罪が起こったときに，IP アドレス以外の方法で攻撃者を特定するため.

3.2　提案手法