

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 を保存するように支持されたブラウザは、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、ショッピングカード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

サイバー犯罪が起こった際に、IP アドレスなどで犯人を特定するが、最近では、キャリアグレード NAT などの技術の普及により、IP アドレスでの追跡は困難となっている。そこで、IP アドレス以外の情報、たとえば Cookie などを用いることで犯人を特定する手法について提案する。

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