1
指導ポイント

ネットは匿名性が高いため、さまざまな問題を引き起こしていると考えられている。「ネットいじめ」や「ブログ炎上」「なりすましメール」などは、すべて匿名性を利用した問題とも言える。これに対して、ネットを実名でしか利用できないようにすべきだ、という主張も有識者の中にはある。実際に韓国では、事実上の実名主義が取られている。

日本ではネットを匿名で利用できるが、このセクションで説明しているように、実際には個人を特定することは容易である。子どもたちに「名前を隠しても調べればすぐバレるんだよ」と教えることで、匿名性を利用した問題の解決が期待できる。

●ネットでは自分を隠して発言する人がいます●

○本節の目的

ネット上における「匿名性」のメリット・デメリットを理解させる。また匿名であることが、悪意を表出させる要因となりうることについて考えさせる。

日本のネットは、ある程度の匿名性が確保されており、これによって個人のプライバシーが守られたり、立場にとらわれずに文章を表現できたり、ときには不正を告発して社会正義を守るといったメリットを享受できる。

しかしながら、匿名であることを利用して、いたずらや悪事を企てるものもいる。匿名であることが悪意に直結するとは言えないが、「誰がやったかわからない」と思い込むことで、潜在的に持つ悪意や残虐性を表面化させている可能性は否定できない。

ネットに限らず、一般的に不特定多数を相手にするコミュニケーションでは、いわゆる「ウケる」発言をして人気を得たいという欲望が発生する。さらに人は、「真実」よりも「そうであったらおもしろい」方を事実として受け止めたがる傾向があり、この相乗効果により、根拠のない風説が真実であるかのように語られることもままある。

2008 年にはネットにおける殺人予告が社会問題化し、匿名掲示板「2 ちゃんねる」の事例だけでも、下は小学 6 年生から上は高校 3 年生までの学生が、軽犯罪法違反（業務妨害）による書類送検や、威力業務妨害で逮捕されている。ただし現在は、いくつかの抑止策や逮捕報道などの結果、こういった事件は減少傾向にある。

悪意の表出に対する 1 つの抑止方法は、これを倫理的な問題として解決することである。人の中にある道徳感や正義感に照らし合わせることで、悪意のある発言や行動を、匿名の状態においても抑止することは可能であろう。ただしこの方法は、残念ながら本人の資質に依存する部分も少なくない。

むしろ技術的な側面から、匿名性がどのように実現されているかを説明する方が、より多くの人に理解されることだろう。次節では技術的な観点から、抑止力となり得るポイントを解説する。

●名前を隠してもログを見ればわかります●

○本節の目的

技術的観点からインターネットは「匿名」ではないことを解説し、本質的な理解への手助けとする。

インターネット上の掲示板やメールにおいて、発信者名が書かれていなかったり偽ってあれば「匿名」であるように見える。しかし、実際にはそのコンテンツをやりとりするために、ソフトウェアや機器同士が接続し、複数のレイヤー（層）間で通信が行われている。

このレイヤーそれぞれに、通信状況が「ログ」として記録・保存されている。例えば掲示板を閲覧すれば、その掲示板が開設されているウェブサーバーにアクセスのログが保存される。これらのログをたどることで、情報の発信者を特定することができる。

ただし、閲覧者の住所や氏名までが、ログに記載されているわけではない。実際に個人を特定するためには、インターネットへの接続を仲介しているプロバイダの協力も必要になる。インターネット接続のレイヤーで記録されているログを、ウェブ通信のレイヤーのログと突き合わせ、専門家による解析が必要となる。

また、こういったログは誰でも見られるわけではなく、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」、通称「プロバイダ責任制限法」に則って、情報開示請求を行う必要がある。この法律の特徴は、下記２点に集約される。

1.　発信者情報の開示請求

特定電気通信（インターネット接続）による情報の流通により、自己の権利を侵害されたとする者は、関係するプロバイダ等に対し、当該プロバイダ等が保有する発信者の情報の開示を請求できる。

2.　プロバイダ等の損害賠償責任の制限

特定電気通信による情報の流通により他人の権利が侵害されたとき、これによって生じた損害について、関係するプロバイダ等が賠償しなくてもよい場合が規定されている。

メールにおける発信者の特定

メールでは、ある程度の情報が「ヘッダ」に記載された状態で届くため、掲示板の書き込みなどに比べれば、発信者の特定は容易である。代表的な携帯電話キャリアで、ヘッダ情報を確認する方法を記載しておく。

・NTT ドコモ

「iMenu」⇒「お客様サポート」⇒「各種設定（確認・変更・利用）」⇒「メール設定」⇒「その他設定」から「メールヘッダ情報受信設定」を選択し「付加する」に設定

※設定した後から受信するメールにヘッダ情報が追加される。パケット代が余分にかかるので注意。メールが全文受信できない場合は、下記設定を変更して全文受信できるようにしておく。

「iMenu」⇒「お客様サポート」⇒「各種設定（確認・変更・利用）」⇒「メール設定」⇒「その他設定」から「メールサイズ制限」（mova では「受信文字数制限」）

・au

「E メールメニュー」⇒「E メール設定」⇒「その他の設定」から「E メールヘッダ情報表示」を選択し、暗証番号を入力。

※過去 30 日間に受信したメールのヘッダ情報を見ることができる。

・SoftBank

まず専用パスワードを入手する必要がある。契約者本人が 157 に電話して、オペレータにパスワード発行の申し込みをすると、パスワードが携帯に届く。有効期限は 10 日間である。次に、SoftBank のウェブサイトにアクセスして「オリジナルメール設定」⇒「E メールヘッダ情報閲覧」を開き、入手したパスワードを入力する。

※過去 2 日間に受信したメールのヘッダ情報を見ることができる。

・ウィルコム

ウィルコムの電話機では、基本的には電話機側でメールヘッダを確認する方法はない。

代替の方法として、オンラインサインアップの転送設定でパソコンのメールアドレスを設定し、パソコンに転送されたメールでヘッダ情報を確認することができる。例えば Outlook Express で受信したなら、閲覧したいメールを展開して「ファイル」⇒「プロパティ」⇒「詳細」⇒「このメッセージのインターネットヘッダー」で参照できる。