

## 事例 D-5

(1) タイトル：大学内ネットワークにおける運用管理とプライバシー

(2) 本文：

あなたは、小さな大学の情報システム課に勤務するシステムエンジニア (SE) 兼ネットワーク管理者である。この大学におけるインターネット接続および関連サービス (教職員向けの電子メールやウェブホスティング) は、あなたが管理している。ネットワーク利用規定や情報セキュリティポリシーは、文系中心の小さな大学ということから、あまり変わったアプリケーションソフトウェアを使う教職員もいなかったため、ごくごく簡単なものであった。また、学生は、パーソナルコンピュータやスマートフォンの MAC アドレスなどを登録すれば、自分の機器を大学の無線 LAN に接続できる。

新年度になって、情報倫理学を研究する O という教員が、あなたの大学に赴任してきた。インターネット技術の詳細にはあまり詳しくはないようだが、「通信の秘密」とか「プライバシー」とかどうも面倒くさいことを初対面のあなたに話しかけてきた。適当に相槌を打って話を合わせていたが、この機会にネットワーク利用規定や情報セキュリティポリシーの整備に力を貸してくれるかなと思う一方で、なんだか面倒くさい男が来たという印象もある。

ある日あなたが昼食から職場に戻ろうと歩いていると、スマートフォンに電話がかかってきた。情報処理担当の教員から、ホームページ制作を学生に行わせていたのだが、ネットワークが異常に遅くなっていて、授業にならないという苦情である。職場に戻り、何が起こっていたのか、ネットワーク管理ソフトウェアで確認すると、通常使われないポートを用いて、大量のデータの受信が行われていることがわかった。ログを調べると、教育発達学部の学生が登録したパソコンから送受信が行われている。

おそらく P2P ファイル共有ソフトを用いて、大量の映像かゲームをダウンロードしていたように思われる。学科長にお願いして、この学生を呼び出してもらい、学生部長にも話して、注意をしなければと考えた。この P2P ファイル共有ソフトはポートを偽装するので、特定のポートを閉じても別のポートを使って通信するかもしれない。本学に導入されているルータは帯域制御機能を有していて、この P2P ファイル共有ソフトのパケットパターンを検知して遮断したり、パケット送信の優先度を下げることができる。

ルータの帯域制御機能をとにかく設定して、この P2P ファイル共有ソフトを遮断してしまうか、パケット送信の優先度を下げようと考えたところで、例の O の顔が思い浮かんだ。突然帯域制御を行って、O がその事実を知ったら、いろいろ

ると面倒臭いことを言うてくるだろうなと考えた。

確かにパケットヘッダを読み取って振り分けることは、通信の秘密に抵触する可能性がある。ところが、通信の秘密を守るよう義務付けられているのは電気通信事業者であるが、大学の情報システム課は電気通信事業者には当たらない。また、ネットワークの円滑な利用を考えれば、帯域制御機能を用いて、P2P ファイル共有ソフトのパケットの送信を制限することには、問題がないだろう。大学のネットワークやそれを構成するルータは大学の財産であって、財産権にもとづく管理権もある。だが、そもそもネットワーク利用規定や、情報セキュリティポリシーで、帯域制御を行うことを宣言していない。また、通信の秘密の遵守は必要がなかったとしても、プライバシー侵害という観点から見た場合、どうだろうか。例の P2P ファイル共有ソフトの送受信データは暗号化されているものの、暗号の実装が失敗しているので、セキュリティツールを使うと、ペイロードを覗くこともできる。電気通信事業者でないとしても、ネットワーク管理者は、パケット監視によってアプリケーションや、場合によってはペイロードの中身を見ることも可能である。

結論としては、P2P ファイル共有ソフトの帯域制御を行って、通信の円滑な利用を実現するべきであろう。0 のようなうるさ方にはどのように説明をすれば良いか。また、どのように手続きを進めれば良いか。

### (3) 考えてみよう。

(1) 2人組になって、主人公のあなた役と 0 役とに分かれなさい。0 役の人は、通信の秘密やプライバシーを重視する 0 の帯域制御を批判する議論を想定しなさい。この場合、どのような理由を用いて帯域制御を批判することになるか、その理由を重視して、主人公役の人に帯域制御批判を行うこと。次に、あなた役の方は、その議論に反論しながら、通信の円滑な利用を実現するために帯域制御を導入すべきだと、理由を示して説得しなさい。

(2) 日本インターネットプロバイダー協会 (JAIPA) のホームページで、帯域制御ガイドラインを探し、プロバイダ (ISP) がどのような根拠から、帯域制御を行っているか確認しなさい。なお、帯域の爆発的な利用からの「緊急避難」の法理は、継続的に帯域制御を利用することから考えると適切ではないとの法学者の指摘がある。この点を考慮すると、プロバイダは、どのような理由から帯域制御をすればよいか考えなさい。

(3) 上記の JAIPA のガイドラインを参照しながら、P2P ファイル共有ソフトやその他のネットワークの混雑を引き起こしそうなアプリケーションの帯域制御を行うにあたって、どのような手続きをおこなえばよいか（ユーザーへの通知やネットワーク利用規定の整備と公開なども含む）、その手順を考えなさい。

(4) 総務省は、ボットなどのマルウェアに感染したルータやパーソナルコンピュータの被害拡大を防ぐため、プロバイダが感染したルータやパーソナルコンピュータのユーザーに対して協力を求めたり、ボットを遠隔操作する C&C サーバーへの通信を遮断するための手続きや条件を定めた。このガイドライン（第二次とりまとめ）を読み、手続きや条件について、簡単にまとめなさい（包括的同意とオプトアウトがポイント）。

(5) 総務省は、パケット監視をもとに、行動ターゲティング広告を行おうとする者に対して、ユーザーに対する通知と同意を定めている（「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会 第二次提言」）。この文書を読み、行動ターゲティング広告におけるパケット読み取り（ペイロードの読み取りも含む）と、マルウェアの被害防止やネットワークの混雑防止のためのパケット読み取りとを比較して、後者と比較して、どうして前者は実施するのにより制限が必要なのか、説明しなさい。

(6) 上記(5)の第二次提言を読み、現実的に見て、プロバイダなど、他人の通信を媒介する者（広い意味では、MVNO・プロバイダなどに加えて、SNS や電子掲示板の管理者も含まれる）は、その都度通知と同意を得ることができるか、どのような通知と同意を行うべきか、(4)の文書も参考にしながら、仲間とともに話し合いなさい。

#### 付属資料

- (1) [事例D-5-1](#)：参考文献

## 事例D-5-1

### 参考文献

- 1)海野敦史「『通信の秘密』不可侵の法理」勁草書房，2015.
- 2)帯域制御ガイドライン運用基準検討協議会「「帯域制御の運用基準に関するガイドライン」の改定について（12/03/30）」

<https://www.jaipa.or.jp/other/bandwidth/info-120330.php>