# 1.2 ネットワーク利用のルールとマナー

## 1.2.1　ネットワーク利用のルールを知ろう

インターネットの普及により私たちは、インターネットに接続されたコンピュータで、いろいろな情報を簡単に手に入れられるようになりましたが、それに伴い、インターネット社会における様々な責任と、ルールを守る義務も発生しました。

また、自分が所属しているネットワークの利用規則や法律に違反する行為は行ってはいけません。自分の行為が適切であるかを正しく判断してコンピュータ・ネットワークを使いましょう。

### ■　高経ネットの利用規則を遵守しましょう

高経ネットは、本学教職員や学生が学術研究、教育活動、大学における様々な事務手続きなどの仕組みを支える情報基盤ネットワークシステムです。高経ネットの利用規則や大学の「情報セキュリティポリシー」を守って、本コンピュータ・ネットワークの運用に支障を及ぼさないようにしましょう。

高経ネットの利用規則や「情報セキュリティポリシー」の詳細は、大学ホームページの情報基盤センターホームページを表示し､「関連規程」で確認することができます。

### ■　法律に違反する行為はしない

#### ◇ 著作権侵害

「著作権」とは、著作権者が無断で他人に著作物を使用されないように保護するための権利で「著作権法」という法律によって保護されています。

著作権侵害は犯罪ですので懲役または罰金などの罰則規定があります。

以下のような行為は、著作権侵害となります。

1. ファイル共有ソフトを利用する。(知らないうちに自分のパソコンが著作権侵害の「違法ファイル」を送信するという違法行為を行うことになります。)
2. 著作権侵害の違法サイトから違法と知りながら音楽や映像をダウンロード（録音、録画）して利用する。(個人利用であっても 2 年以下の懲役または 200 万円以下の罰金が科せられます。また、令和 3 年 1 月 1 日から、ダウンロードの規制が、音楽・映像から全ての著作物に拡大されました。)
3. 友達が購入したソフトウェアの CD を借りて、自分のパソコンにインストールする。(ソフトウェアは著作物であり、使用許諾契約等が結ばれています。)
4. Web ページなどに掲載されている文章や論文、画像をそのままコピーし、自分のレポートに利用して提出する。

なお､著作権法では､著作権者に無断で著作物を利用してもよい例外もいくつか認められています。

1. Web ページで見た情報を印刷してじっくり見たい・自分の CD からベストコレクションを作りたいなどの個人利用の場合、複製することは問題ありません。
2. 「自分の論文に Web ページで公開されている論文の一部を使いたい」というときなど、引用のルールを守れば、著作権者に許可なく著作物を利用することができます。

### 1-12　引用のルールとは？

著作権法で明確に引用の「ルール」が示されているわけではありませんが、次の点に気をつければ問題ないでしょう。

- 引用部分を明示すること。（括弧やインデントなどで本文とは違うことをはっきりさせる）
- 引用部分の出所を明示すること。（Web ページの場合は URL などを記入する）
- 引用部分は質的にも量的にも本文に比べて「従属」するもので、引用する必然性があること。

## ◇ 不正アクセス

「不正アクセス行為の禁止等に関する法律」（不正アクセス禁止法）は、不正アクセス行為の禁止・処罰を対象としたもので、次のような行為は「不正アクセス行為」や「不正アクセスを助長させる行為」として禁止されています。

1. 他人のユーザ ID・パスワードを無断で使用する行為。
   また、他人のパスワードを無断で第三者に提供する行為。
2. アカウントのないコンピュータに、セキュリティホールなどを攻撃して直接的にまたは間接的に侵入して不正に利用する行為。

なお、さらなる対策強化のため平成 24 年 5 月には改正法が施行され、「ID やパスワードを不正に要求する行為（フィッシング行為）」も処罰の対象となりました。

### 1-13　なりすまし-SNS でも注意しよう

他人のパスワードを盗んでその人になりすましてメールを送信したり、Web ページを変更したりする行為は「不正アクセス禁止法」で禁止されています。また、ユーザ ID・パスワードを貸し借りしたり、記載した紙を紛失したりするなど管理がずさんでなりすまされた場合は、本人の管理義務の責任が問われます。

X（旧 Twitter）や Facebook、LINE に代表される SNS(Social Networking Service)についても、なりすましの脅威が高まっています。むやみに個人情報を入力することは避け、個人情報を開示する範囲についても良く考えて設定しましょう。

### 1-14　ボットに感染して不正アクセスに加担？

ボット（BOT）とは、コンピュータを外部から遠隔操作するためのコンピュータウイルスで、これに感染するとそのコンピュータはボットネットワークの一部に組み込まれ、悪意のあるハッカーに遠隔操作され、持ち主が知らないうちに「迷惑メールの配信」や「インターネット上のコンピュータへの攻撃」など迷惑行為や犯罪行為に利用されてしまいます。

知らないうちに「不正アクセス」に加担していたなどということがないように注意しましょう！

## ◇ その他の法律違反となるような行為

以下の行為は、法律違反行為となります。違反者は、法的に処罰されますので注意しましょう。

1. 有害情報（わいせつ・暴力など犯罪に繋がる情報等）を Web ページで公開する。
2. 著作物（写真・絵・文書等）を Web ページ上で無断掲載したりする。
3. 他人を誹謗中傷する内容を Web ページに公開したり、掲示板に書き込んだりする。
4. 他人のメール・写真等を無断で Web ページに公開したり、掲示板に書き込んだりする。
5. 「ねずみ講」まがいの Web ページを公開する。

## ■　電子メール利用のマナー＆注意事項

### ◇ メール送信

電子メールを送るときには次のようなマナーと注意事項を守り、相手に迷惑をかけないようにしましょう。

1. メールアドレスを間違えないようにする。
   大学メール（Microsoft 365）では、送信前プレビューで送信アドレスをチェックしてからでないと送信できません。
2. 基本的には、メールはテキスト形式で送信する。
   HTML メールは、**マルウェア（コンピュータウイルス、スパイウェア、ボットなど悪意のあるプログラム）**が組み込まれやすいため、受信者によっては受け取りを拒否される場合があります。
3. メールの「Subject（件名）」は必ずつける。
   メールの題名から内容が推測できるように、一目で分かりやすい題名をつけたほうが親切です。
4. サイズの大きい添付ファイルをつけて送る場合は、事前に確認する。
   メール受信側の環境では、大きな添付ファイルは受け取れない場合があります。

### ◇ メール受信

電子メールを受け取ったときは、次のようなことに気をつけましょう。

1. メールの添付ファイルを安易に開かない。
   メールに添付されたファイルにはウイルスが潜んでいる可能性もあります。安易に添付ファイルを開かないように注意しましょう。
   最近のウイルス感染を狙ったメール（標的型攻撃メール）は、組織や個人に合わせて標題やメールの内容がカスタマイズされているので、標題や内容を見ても怪しいなメールと判断できず、添付ファイルをつい開いてしまい、ウイルスに感染するなどの被害が発生している。
2. 本文中のリンクは安易にクリックしない。
   送られてきたメールが偽メールである可能性もあります。本文中のリンクを安易にクリックして、マルウェアや不審なプログラムを配布するサイトやフィッシング詐欺サイトに誘導され、ID・パスワードを盗まれるなどの被害に遭うことにもなりかねません。

## ■　Web ページ閲覧・公開時のマナー＆注意事項

### ◇ Web ページ閲覧

インターネット上では様々な Web ページが公開されています。次の点に注意して閲覧しましょう。

1. 正規のサイトでも要注意！
   公開されている Web サイトの中には、外観上正常なページと変わらない正規の Web サイトが改ざんされ不正サイトに誘導する仕掛けが埋め込まれているケースがあります。有害サイトや不正サイトにはアクセスしただけで、自動的にマルウェア送り込まれてくるように仕組まれている場合があります。
2. 不用意に個人情報を入力しない。
   Web 上でアンケートや通信販売を行うサイトがありますが、このようなページに回答するだけでも「個人情報を公開する」ことになります。「個人情報」である、氏名や年齢、住所・電話番号などはもちろん、すぐに自分には結びつかないと思われる情報でも、送信する際はよく考えてから行いましょう。インターネット上に送信された情報は、簡単にコピーされて広まり、簡単に回収できなくなります。

### 1-15　Web ページの閲覧制限

Web ページ情報の中には、学術研究・教育のためという学内コンピュータ・ネットワークの利用目的に反する情報を提供するサイトがあります。学内ではそのようなサイトについては、フィルタリングソフトによる一部閲覧制限を設けています。

## ◇ Web ページ公開

本学では、研究室、ゼミ、学生団体などが申請手続きに基づいて、Web ページを公開することができます。

1. 個人の Web ページは公開できません。
   ただし、授業の課題で個人ごとに作成したものは、担当教員の責任の下に公開することが認められています。
2. 個人情報に注意する。
   Web ページを公開すると様々な人が閲覧します。中には悪意に満ちた人がいる可能性も否定できません。個人が特定できる情報の掲載は極力さけましょう。
3. 著作権や肖像権に注意する。
   他人の Web ページからダウンロードした画像や写真を、勝手に自分の Web ページに貼り付けて公開してはいけません。作成者本人の著作権や写真に写っている本人の肖像権など、当事者の了解なしに利用することはできません。

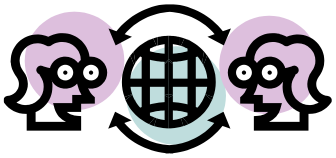
### 1-16　SNS によるプライバシーや情報漏洩に関する注意

X（旧 Twitter）や Facebook、LINE などの SNS は、自分の友人・知人とのやりとりが多いため、ごく狭い世界で情報を書き込んでいると誤解しがちです。しかし実際には、自分の書き込みを全世界に公開する設定になっていることに大部分の人が気づいていません。

X（旧 Twitter）は、他人の書き込み（ツイート)内容を検索することができます。また他人の書き込みを再書き込み(リツイート)して別の人に教えることもできるため、“くちコミ”のように連鎖式に多くの人に広まってしまう脅威があります。

安易な書き込みが元で、就職の内定が取り消されたり、アルバイトを解雇されたりというニュースも多く聞かれます。インターネット上に一度でも書き込まれた情報は半永久的に残ってしまい、削除が容易ではありません。

自分自身の書き込みに気を付け、匿名性に驕らず、普段の生活と同じく、責任ある行動や発言を心掛けましょう。



## 1.2.2　インターネットのトラブルにご用心

インターネットの普及に伴って、インターネット上の被害やトラブルも急増しています。どのようなトラブルがあるかを知り、そのようなトラブルに自分が巻き込まれないように注意しましょう。

### ■　マルウェア（Malware）被害

マルウェアとは、コンピュータウイルス、トロイの木馬、ワーム、スパイウェア、ボットなどの悪意のあるプログラムの総称です。

**コンピュータウイルス**は、他のファイルやソフトウェアに寄生して悪さをするソフトウェアのことです。寄生せずに自分自身を複製して増殖し、ネットワークを這い回り脆弱性のあるマシンに侵入するタイプの**ワーム**や、有益なプログラムのふりをして知らないうちに不正な行為を行う**トロイの木馬**と呼ばれるものがあります。

**スパイウェア**は不正にユーザの個人情報などを収集するプログラムです。収集した情報を外部に送信する機能を持つものもあり、情報漏洩につながる危険性をもっています。

**ボット**はウイルスの一種で、ユーザのコンピュータに感染し、ネットワークを通じて感染したコンピュータを外部から操る目的をもつプログラムです。ボットに感染したコンピュータは、外部から与えられた指示に従って不正な行為を行います。


【被害状況】

マルウェアに感染すると、様々な被害を受けてしまいます。

1. 情報漏洩

   P2P ファイル交換ソフト経由で感染を広めるウイルスに感染すると、パソコン内にあるデータやデスクトップ画面などが、本人が気づかないうちに P2P ファイル交換ソフトの「公開用フォルダ」へ勝手にコピーされ、ネットワーク上に流出します。

   山田オルタナティブというウイルスに感染すると、感染したパソコンの全ファイルを丸ごとネットワークに公開してしまいます。

   キーロガーというスパイウェアに感染すると、ネット銀行の口座番号や暗証番号などの情報を盗まれます。

2. 不正サイトへの誘導やマルウェアのダウンロード

   感染したコンピュータが勝手にインターネットにアクセスして、別のマルウェアを次々にダウンロードし、不正実行機能をバージョンアップしていきます。また、ブラウザを乗っ取って不正サイトに誘導したり、意図しない検索結果を表示したりするスパイウェアも見つかっています。

3. DDoS 攻撃への加担

   ボットに感染した数千から数万のコンピュータを踏み台にして、標的とするコンピュータに一斉に攻撃を仕掛けて機能停止に追い込んだりすることを DDoS(Distributed Denaial of Service:分散型サービス妨害攻撃)といいます。このウイルスに感染すると、そのことに気づかずに DDoS 攻撃加担してしまうこともなります。

4. ウイルスメールの大量送信や差出人アドレスの詐称

   ウイルスに感染すると、ウイルスが勝手にコンピュータ内にあるメールアドレスを探し出し、このアドレスを利用してウイルスメールを送りつけます。このとき差出人、件名を詐称してユーザの錯誤を誘います。ユーザは知人からのメールやエラーメールと勘違いしてメールの添付ファイルを開き、感染してしまいます。

5.　ウイルス対策ソフト停止やベンダーWeb サイトへのアクセス妨害

感染すると、ウイルス対策ソフトウェアの機能を停止させるウイルスがあります。また、セキュリティ対策ソフトメーカーの Web サイトにアクセスさせないように妨害するウイルスもあります。

6.　パソコン機能停止

感染すると、今まで無事に使えていたコンピュータが急に再起動を繰り返して使えなくなるという事象があります。ウイルス活動のためコンピュータが不安定になり、再起動が繰り返し実行されるのです。さらにデータファイルを破棄したり、コンピュータを起動できなくしたりなどの被害をもたらすものもあります。

【感染原因】

マルウェアは、次のような何らかのきっかけとなるユーザの操作を利用してコンピュータに入り込み、感染します。

1.　USB メモリの接続

USB メモリ感染型ウイルスは、USB メモリが接続された際にその中にあるプログラムを自動実行する機能を悪用したものです。感染すると USB 内に Autorun.inf という隠しファイルを作成し、ウイルスが自動実行される状態になりパソコンに感染します。

2.　ネットワークへの接続

ウイルスはネットワークに接続しているコンピュータの中から、特殊な信号を発信して（ポートスキャンをかけて）脆弱性のあるコンピュータを探します。脆弱性のあるコンピュータを発見するとウイルスを送り込みます。またパスワードの設定が甘いネットワーク上の共有フォルダに、パスワードを破ってアクセスし、ウイルスを書き込みます。

3.　Web ページの閲覧

ブラウザに脆弱性があると、Web ページを見るだけで感染することがあります。攻撃者は特定の Web ページを改ざんし、マルウェアを仕掛けたりします。そのような Web サイトをウイルス対策がされていないパソコンで閲覧するだけで感染してしまうのです。

4.　メールの開封やプレビュー

メールソフトや OS に脆弱性があると、メールを開いたりプレビューしたりするだけで添付ファイルが実行され、感染してしまいます。

5.　添付ファイルのオープン

ウイルスは様々な経路で届きますが、よく悪用されるのがメールの添付ファイルで届くケースで、添付ファイルを開くとウイルスが活動し感染します。このタイプのウイルスは、ファイルを開かなければ感染しませんが、ユーザの気を引くようなファイル名をつけたり、ファイルの種類を特定する拡張子を偽装したりしてユーザがうっかり開いてしまうような巧妙な手口を使います。

【対策方法】

マルウェアの侵入を防ぐには、次のような対策、常日頃から心がけておく必要があります。

1.　脆弱性の解消

OS やソフトウェア（Web ブラウザやメールソフトなど）に脆弱性があるとそこを突破口にしてマルウェアに感染したり、攻撃をうけたりすることがあります。脆弱性を解消するために、Windows アップデートやソフトウェアのバージョンアップ等を定期的に行い、セキュリティ対策をしておきましょう。

2.　ウイルス対策ソフトウェアのインストールと更新

ウイルス対策ソフトウェアは、ファイルやディスクを検査して、ウイルスが見つかるとウイルス名や感染ファイル名を表示してくれます。ウイルス対策ソフトウェアは、パターンファイル（ウイルス定義

ファイルともいう）を使用してウイルスを検出しています。パターンファイルは定期的に更新をして最新のウイルスが検知できるようにしておきましょう。

3. パーソナルファイヤーウォールの活用

インターネットに接続されているパソコンは、常にウイルスの感染や不正アクセスの危険にさらされています。ファイヤーウォールを正しく設定・運用することで、脆弱性を悪用した不正プログラムの侵入に警告を表示し、侵入を防ぎます。また、侵入したスパイウェアやウイルスなどの外部への情報発信も防ぐことができます。

ウイルス対策ソフトウェアには、パーソナルファイヤーウォール機能を持つものもあります。

**1-17　大学提供ウイルス対策ソフトを活用しましょう**

大学では無償で「McAfee ウイルス対策ソフト」を学生の皆さんに 1 ライセンス提供しています。情報基盤センターホームページの「ウイルス対策ソフト」のページで確認してください。

https://www3.tcue.ac.jp/jouhou/list/common.html（学内専用ページです）

## ■　フィッシング（Phishing）詐欺被害

フィッシング詐欺とは、銀行やクレジットカード会社、ショッピングサイトからのメールを装って、偽りの Web ページにアクセスさせ、「クレジットカード番号」や「ユーザ ID やパスワード」を入力させて盗むという詐欺行為です。盗まれた情報は自分が被害を受けるだけでなく、オンラインショップやオークションなどで悪用され、別の利用者をだますことに使われることもあります。

【巧妙な手口】

ユーザ゛をだますためにさまざまな工夫が凝らされています。典型的な手口は「ユーザを錯誤させる騙しメールの送信」、「本物に見間違えるような偽サイトへの誘導」、「個人情報の入力を求める」などです。

【対策方法】

ただのメールが送られてくるだけで、添付ファイルもなく、ウイルス対策ソフトで検知されるわけではありません。防ぐためには、次の点に気をつけましょう。

- メールの送信元を安易に信用しない。
- 送られてきたメールの内容を安易に信用しない。
- メールのリンクを安易にクリックしない。
- 入力前に本物のサイトかどうか確認する。
- メールからアクセスしたサイトに安易に個人情報を入力しない。

**1-18　本物のサイトか確認する方法**

・アドレスバーに正しい URL が表示されているか確認する。
・SSL 接続を示す URL（https://）と鍵アイコンがつながっているかどうか確認する。
・フィッシング対策用のソフトウェアを使用する。

## ■　迷惑（スパム）メール

知らない人や会社などから、営利目的で、無差別・大量に送りつけられてくる宣伝メールを一般的に「迷惑メール」または「スパム（spam）メール」といいます。スパムメールには、宣伝広告メール、勧誘メールだけでなく、架空請求メール、フィッシング詐欺メールなどがあり、騙されないように注意する必要があります。

迷惑メールは、Web ページやオンラインアンケートで入力したアドレスが漏れたり、個人情報の流出などでアドレスが悪徳業者間で売買されたり、適当に文字列を組み合わせて作られたアドレスがたまたま届いてしまったなどの理由で送られてきます。

【対策方法】

- スパムメールは無視し、絶対に返事を出さない。
- 本文中に書かれた電話番号に電話したりしない。
- スパムに書かれた URL にアクセスしない。
- Web ページ上でのメールアドレスの掲載は控える。

**1-19　迷惑メールフィルタの利用**

高経ネットでは、ネットワークの仕組みとして迷惑メールをブロックするなどの対策を行っており、毎月受信メールの多くのメールがブロック対象となっています。それでも、中にはブロックされずにメールボックスに受信されてしまう迷惑メールがあります。
大学メール（Microsoft 365）にも迷惑メールの振り分けができる「迷惑メールフィルタ」機能がありますので、設定方法を確認しておくとよいでしょう。
なお、時々正しいメールが誤って迷惑メールと判断されてしまう場合もありますので、**迷惑メールフォルダ内も定期的に確認しましょう。**

## ■　ワンクリック詐欺

ネットサーフィンをしているときなどに、Web ページに表示された画像やアイコン、リンクなどをクリックしただけで有料サイトに入会登録したとみなす画面を表示し、払う必要のない料金を請求する詐欺です。

ワンクリック詐欺のサイトへの誘導手口はスパムメールのリンク、有害サイト（出会い系、アダルトサイト）へのリンクだけでなく、一見まともなブログや掲示板中のリンクなどにも存在し、そこをクリックすると料金請求画面のページが表示されます。また、料金請求画面でなくウイルスがダウンロードされ埋め込まれる場合もあります。

【対策方法】

- 好奇心から有害サイトにはアクセスしない。
- 料金請求メールがきても、絶対に料金を払わないで無視する。また、相手に連絡をしない。
- ウイルスを埋め込もうとすると Windows のセキュリティ警告がでるので、その警告を無視しない。
- 怪しいプログラムは実行しない。
- 万が一のため、そのサイトの URL や画面を印刷しておく。

注意）高経ネットおよび発行されたアカウントは、学術研究・教育目的以外での利用を禁止しています。

### ■　オークションサイトでの詐欺


インターネットを利用したオークションでは、中古品ばかりでなく、新品商品なども自宅で気軽に安く売買を行うことができます。しかし、購入した商品が届かなかったり、逆に商品を発送したにもかかわらずお金が振り込まれなかったりなどの詐欺被害が多く発生しています。

オークションを利用する際には、これらの危険をきちんと考えて対応しましょう。

【対策方法】

- 出品者の評価を参考にする。
- 代金引換などの安全な取引をする。
- 取引相手の住所や電話番号を必ず確認する。
- オークションページや入札履歴を印刷し、取引の内容を保存しておく。

注意）高経ネットおよび発行されたアカウントは、学術研究・教育目的以外での利用を禁止しています。

## 1.2.3　モバイル端末の利用にご用心

この数年に間に、スマートフォンやタブレット型端末などのモバイル端末の利用がかなり進んでいます。パソコン並みの高い性能を持ちながら持ち運びに優れていることが最大の特徴です。

しかし、さまざまな用途に利用できて便利な反面、リスクも存在します。セキュリティの観点からリスクをきちんと理解し、対策を講じてください。

### ■　モバイル端末の危険性

1. 端末には大量の情報が保存

   モバイル端末には、電話番号やアドレス帳、端末情報が保存されていますが、その他にも、次に示すような多くの情報が自分でも知らない内に蓄積されていきます。

   - メールアドレスのアカウントやパスワード
   - ブラウザなどに登録されたアカウントやパスワード
   - 閲覧記録
   - 位置情報(GPS 機能)
   - 通信記録(オンライン決済情報など)

   使用するアプリによっては、これ以外のデータも保存されています。

2. モバイル端末を狙ったウイルス

   スマートフォンやタブレット型端末を狙ったウイルスやマルウェアが急激に増加しています。

   感染原因はパソコンと同じく、メールやアプリケーション、不正サイトへの接続が主な原因です。ウイルスの機能としては、端末情報（OS のバージョン、電話番号、メールアドレス等）を盗む、別のウイルスを呼び込む、通話内容を記録するなどがあり、ワンクリック請求を行うウイルスも発見されています。

3. 脆弱性の存在

   スマートフォンにも脆弱性が発見されました。それを放置したままにすると、アプリのインストール時に許可した機能以上のことが可能になる危険性があります。勝手に電話が発信されたり、位置情報が漏洩されたりするなどの被害が生じる恐れがあります。

## ■　セキュリティ対策

1. 必ずパスワードを設定し、盗難・紛失に備えましょう
   スマートフォンやタブレット型端末は持ち運びが容易であるため、紛失や盗難の危険性がより高くなります。必ずパスワードを設定し、紛失・盗難時のリスクを軽減しましょう。
   クラウド上のストレージサービスなどで、データを共有している場合、クラウド上のデータや自宅パソコンも情報漏えいの脅威にさらされることになります。紛失や盗難には十分注意してください。

2. セキュリティ対策ソフトを導入しましょう
   タブレット端末にも、パソコンと同じように不正サイトや不正アプリを回避してくれるセキュリティ対策ソフトを導入しましょう。

3. 不用意なインストール、身元不明の怪しいアプリはインストールしない
   アプリは、ユーザからの評価を参考にし、ダウンロードする際に表示される「許可」内容を良く読んでインストールしてください。ユーザが同意すれば、「位置情報」や「個人情報」を収集することを可能にしてしまいます。

4. OS やアプリのバージョンアップは速やかに行う
   パソコンと同様に OS やインストールされたアプリに脆弱性があると、不正プログラムの侵入を回避しにくくなります。

5. Wi-Fi の自動接続を無効にして、不正な侵入は回避しよう
   ネットワークの自動接続を ON にしておくと、セキュリティの設定がなされていないネットワークに自動的に接続してしまい、不正に侵入され、個人情報などを搾取されるなどの危険性がでてきます。

### 1-20　インターネットのトラブルに関する関連機関

- ウイルス対策関連
  「情報処理推進機構（IPA）セキュリティセンター」
- 犯罪関連
  都道府県警察本部サイバー犯罪相談窓口連絡先一覧
  「インターネット安全・安心相談」（警察庁）
- 商品やサービスの購入などに関する消費生活関連
  「消費生活センター」「国民生活センター」連絡先一覧
- インターネットのセキュリティ対策関連
  インターネット・セキュリティ・ナレッジ（トレンドマイクロ）
  「国民のための情報セキュリティサイト」（総務省）：