ヒカリ＆つばさの
情報セキュリティ
３択教室

＜２０１８年版＞

岡田　仁志　編著

国立情報学研究所

目　次

まえがき

大学生なら，だいたい，スマホとかネットを使っているし，パソコンでレポートなんて当たり前ですね。インターネットでは，いろんな情報が手に入るし，会わなくても，どこかの人と遊んだり，買い物できて便利だから，みんな使ってるけれど，あぶないとかいう話も聞くので，気になってるって人のために，この本を作りました。新しい技術は難しくてわからないし，危険という話もよく耳にするので怖いと思っている，もうちょっと年上の方にも読んでいただきたいと思います。

書いたのは，ネットでのトラブルの防ぎかたとか，そのための法律やルールの作りかたを研究している人たちのグループです。大学の先生もいるし，会社の人もいます。このグループで，ずっと前から，ネットワークの利用や運用のガイドラインを提言したり，大学の規則のサンプルを作ったりしてきましたが，今年は大学生にわかってほしいチェックポイントを説明する文書を書こうと考えて，１８の話題をえらんで，三択クイズを考えました。

ネットを家でも大学でも使うし，スマホでも使う人は，様々な危険にぶつかるリスクがあります。使っている人やコンピュータが危ない目に会う問題を情報セキュリティと言います。大学では，いろんな人が出入りするし，さまざまなパソコンやシステムを使うし，友達からいろんな使い方を教わることもあるので，大学で規則を定めるだけでは情報セキュリティ対策は難しいですし，実際に被害にあった学生がいるという大学もよく聞きます。この本は法律や技術の難しい話をできるだけ避けて，問題と対策だけに集中しているので，一通り眺めてみてください。

大学の先生へ

本書は，大学生などの情報セキュリティリテラシを未修得のまま情報サービスやインターネットを大いに使っている層を想定して，情報セキュリティ対策のための教材として執筆しました。講義資料の参考としたり，学生向けの補助教材として使ったりすることも可能と思います。対策のお役にたてれば幸いです。

2017 年 10 月　青葉山にて
著者の皆さんに代わり　曽根秀昭

この本の使い方

この本は，全部で17話からなる情報セキュリティ教材です。4人の大学生をめぐる17種類の場面に関わるクイズを解いていくうちに，自然に情報セキュリティの知識が身につきます。

●クイズと解説
クイズの次ページに答が書いてありますが，まずは見ずに考えてみてください。正解・不正解に関わらず，ひととおり解説を読むことで，情報セキュリティ対策をしないことによるリスクや，具体的な対策の方法について学ぶことができます。

●コラム
コラムでは，それぞれの場面におけるリスクや対策に関するやや高度な内容を扱っています。興味に応じて参考にしてください。

本書を教材として利用する場合のルールを135ページに示しています。

登場人物

しずか

クラブ活動に夢中で，大学紹介冊子の取材でヒカリと知り合う。テニス部の副キャプテンで，面倒見がよく部内のみならず，他大学の選手から厚い信頼を寄せられている。新入生勧誘のためのクラブのホームページ作りをきっかけに，コンピュータに詳しくなり，ヒカリの様々な疑問を丁寧に解説する。

ヒカリ

神戸出身の令嬢で，某女性ファッション誌の読者モデルの最終選考まで残ったことがある。趣味は海外旅行と買物で，両親とは何でも話せる仲だ。家電製品の取扱説明書を最後まで読むことが苦手で，使い方でわからないと，ついしずかに頼っている。 しずかの試合の応援には必ず行く勝利の女神。

登場人物

ケイタ

仙台出身で，高校生の時から写真の腕前は有名で多くの賞を受賞している。撮影した写真を快適に処理できるコンピュータが必要になったことがきっかけで詳しくなり，自身のホームページに掲載している鉄道写真は人気が高い。撮影スポットなどの貴重な情報をつばさから教えてもらい，撮影に出かけている。

つばさ

高校時代の友人たちとの幅広い人脈で，毎週のようにコンパに参加して帰宅が遅くなり，両親から度々小言を言われている。ゼミ報告の準備やコンピュータに関することはいつもケイタにお世話になっている。 広い人脈で貴重な情報をケイタに教えることもあって，やんちゃなところがあるが憎めないキャラ。

アプリやゲームの規約読んでますか？

第１話

「同意」ボタンが 表示されたけど…

ヒカリちゃんが，話題のネットゲームで遊びはじめました。使いはじめるときに名前とメールアドレスを入力して「同意」ボタンを押しました。その直後から大量の広告メールが届きはじめたようです。

さて，ここで３択問題です。考えてみてください。

【問題】　ヒカリちゃんは，遊び始める前にどうすればよかったのでしょう？	
A	本名でない名前を入力して「同意」する。
B	友だちに使っているか聞いてから「同意」する。
C	「同意」を押す前に説明をしっかり読む。

この場合のヒカリちゃんの選ぶべき答えは

C 「同意」を押す前に説明をしっかり読む。

です。

どうして<C>なのですか？

アプリやサービスには，利用条件の説明や注意書き，契約書が付属しています。そこには，使用許諾条件，課金条件やダウンロードやインストールに際して必要なことがらが書かれています。そして，それらを読んだ後に「同意」ボタンをクリックすることが使用の前提になっています。ソフトウェアやサービスによっては契約書を最後までスクロールして「同意」ボタンをクリックしないとダウンロードやインストールを開始できないものもあります。

ヒカリちゃんのこのゲームの場合，説明に，「名前やメールアドレスを広告メール配信に利用する」ことや，「集めた情報を第三者に提供する」ことに「同意」すると書いてありました。説明書や契約書をしっかり読むことが必要です。

どうして<A>は間違いなのですか？

実在の名前でなくても，入力したメールアドレスが実在のものなら広告メールは届きます。

どうして<B>は間違いなのですか？

友だちが使っているからといって，説明や契約内容を読まないでアプリやサービスを利用開始することは危険ですから，<B>も不適切です。

「同意」ボタンを押すことは，契約内容に合意したということです。大事な事柄が細かい文字で最後の方に細かい文字で書かれていたり，わかりにくい文章で記載されていたりすることがあります。それらを見落として「同意」を押すと不利な条項も含めて受け入れたことになります。会員制のサイトでは，退会ができないサイトがあったりします。とんでもない金額をサービスに支払うことになるとか，怪しいソフトウェアをインストールされることもあります。そのような事柄も契約書に記載されているはずです。

ヒカリちゃんは，どうすればよかったの？

アプリやサービスを使い始めるまえに，契約書や説明書をしっかり読みましょう。読んでみて，少しでも怪しいなと感じたり，内容に疑問が残るようなアプリやサービスは，それが，たとえ話題になっているようなものでも使わないことです。ですから，正解は<C>です。

コラム１-最近のスマホアプリ-

多くのサービスがウェブやスマホのアプリで提供されるようになっています。その中で，特定のゲームが流行すると類似の不正アプリが出現します。スマホのアプリでは，アプリの機能とは無関係なのに連絡帳の情報やプライバシーにかかわる情報にアクセスするものが数多くあります。

大学生をターゲットとして，大学生向けに大学システムの ID とパスワードを入力させるアプリがあります。そんなアプリは便利そうでも使ってはいけません。本来の機能と無関係に，成績などの情報を覗き見される危険性もあります。

コラム２-無料アプリの問題-

無料アプリやゲームでは，課金しないと楽しめないとか，ランダムに表示される広告によって不愉快な思いをすることがあります。また，広告がアプリの操作ボタンと押し間違えやすい，とても紛らわしい位置にランダムに表示され，そこにうっかりタッチすると無関係なゲームのインストールに誘導されることもあります。

広告の表示なら不快ですみますが，プライバシーに関わる情報をサーバに送るものがあります。無料のアプリやサービスは，収集した情報を売るとか大量の広告表示や有料アイテム（ガチャとか）から利益を得ていることが多いのです。

契約書の中身の理解は大事

どのような形式であれ，契約書は大事です。いったんサインアップしてしまうと，自分に不利なことがらが発生しても，「見落としていたから」といった理由で逃れることはできません。また，契約書が日本語でなく内容が理解できない場合には，「同意」すべきではありません。

そこにどのような内容が書かれているか理解できないことがらに同意することは無謀です。

ネットワークプリンターにご用心！

第２話

わけのわからない文字が大量に！

ケイタくんとつばさくんがバス停で話しています。ちょっと聞いてみましょう。つばさくんのゼミにはインターネットにつながったプリンターがあって，レポートの提出に便利らしいです。そのプリンターは買ったままの状態で使われているとか。つばさくんは，そのプリンターの管理をまかされています。そのプリンターに，ある日突然，わけのわからない文字の紙が大量に印刷されました。ゼミのプリンターの管理，どうすればよかったでしょう。

さて，ここで３択問題です。

【問題】	つばさ君は，本当はどうすればよかったのでしょう？
A	ゼミ内からしか使えないように設定しなおす。
B	故障かもしれないのでプリンターの電源を入れなおす。
C	実害はないので無視する。

この場合のつばさ君の選ぶべき答えは

A　ゼミ内からしかアクセスできないように設定しなおす。

です。

どうして<A>なのですか？

IoT（Internet of Things，「もの」のインターネット）時代においては，あらゆるものがインターネットにつながるようになりました。その一方で，IoT 機器にはセキュリティ的に脆弱なものも多く，インターネットにつながっていると機器の内蔵ソフトが外からの攻撃により改変されたり機器が乗っ取られたりすることがあります。ネットワークプリンターやウェブカメラ，ネットにつながるテレビなどが外部から何者かに遠隔操作され，さらには迷惑メールの送信に使われたり DDoS（分散サービス不能攻撃）攻撃に使われる例があります。買ったままの状態で使っているNAS(Network Attached Storage，ネットワーク共有ディスク)装置がウイルスに感染するとか，重要な情報が持ち去られる例も報告されています。

<B>はどのくらい危ないのですか？

誤動作やデータの作成の誤りであれば，電源を入れなおして治ることがあります。しかし，外部から悪用されている場合の対策としては不適切です。

実害はないし<C>じゃだめなんですか？

論外です。外からプリントできるということは，他の設定も脆弱で，ファームウェアの更新もなされていないでしょう。そのような機器が直接ネットワークにつながったままだと，外から乗っ取られかねません。共有ディスクのような情報を保管する機器の場合は重大な情報漏洩を引き起こすこともあります。

つばさ君は，どうすればよかったの？

ネットワークプリンターや共有ディスク等の機器をインターネットから簡単に使えないように，ID とパスワードで保護しましょう。パスワード等は買った時のままではなく，ちゃんと設定をしてください。さらにルータで外から機器を使えないようにアクセス制限をすることも考えましょう。

これらの対策に加えて，定期的にファームウェア等の更新を実施してください。古くなってファームウェアの更新がされなくなった機器は買い替えを考えましょう。一般に設計の新しいものほど高性能でセキュリティへの配慮もされています。

用語解説　「DDoS」

DDoS は Distributed Denial of Services の略です。日本語では分散サービス不能攻撃と呼びます。特定のサイトやネットワークに大量のパケットを送り付け正常なサービスを妨げる攻撃のことです。昨今では，ペタバイト級の大量データを送り付ける攻撃も発生しています。近年は，乗っ取られたウェブカメラやネットにつながったテレビが攻撃元になっています。

コラム１-IoT機器は買ったままで使わない-

IoT機器を購入したままの状態で使うのは危険です。それらの設定情報はウェブブラウザで変更できるのが普通です。そのマニュアルもネットに公開されているので，機器管理用のIDやパスワードがわかることがあります。
機器を買ったら，まず管理用の ID やパスワードを推測しにくいものに変更します。ファームウェアの更新もやっておきましょう。パスワードが電源オフで初期値に戻る小型のセンサー等では，電源オンの都度パスワードの変更を忘れないようにしましょう。

コラム２-パスワードで安心してはいけません-

パスワードで一安心という時代は終わりました。一部のウェブカメラなどは製品出荷時から何者かが遠隔操作できてしまうというような話もあります。価格だけで機器を選ぶのではなく信頼できるメーカーの製品が安心です。

システムはいつも最新に

第３話

古いパソコンを使ってもだいじょうぶ？

つばさくん，古いパソコンを大切にとっておいたようですね。資源保護には貢献しそうですが，ソフトウェアに関しては，そういうわけにはいきません。久しぶりに電源を入れてクラブの名簿を作るのに使おうとしていますが，このまま使ってもだいじょうぶでしょうか？

さて，3択勝負です。

【問題】　久しぶりに電源を入れた古いパソコン，このまま使ってもだいじょうぶ？	
A	ソフトウェアなどを最新の状態にアップデートしてから使う。
B	サポートがきれているが，旧式のソフトウェアは長年使われてきているので安心して使用できる。
C	古いパソコンをあきらめてネットカフェのパソコンを使う。

この場合，つばさくんの選ぶ答えは

A ソフトウェアなどを最新の状態にアップデートしてから使う。

です。

どうして，<A>なのですか？

OSも含めてソフトウェアに欠陥はつきものです。欠陥が入り込まないようにプログラムする努力はされていますが完全ではありません。セキュリティ上の欠陥を利用してウイルス感染などが起ります。OSやソフトウェアを新しいバージョンに入れ替えることをバージョンアップといいます。大幅な改良や新機能の導入などが盛り込まれたアップグレード(メジャーアップデート)とセキュリティ上の欠陥などを修正したセキュリティフィックスがあります。古いソフトウェアでもサポートが継続されていて，きちんとアップデートしたソフトウェアが提供されていれば使い続けても大丈夫です。

どうして，<B>と<C>は間違いなのですか？

<B>の使い慣れたソフトをそのまま使い続けることは，気分的には安心でも危険がいっぱいです。OSやソフトウェアは，不具合の改良やセキュリティの欠陥をなくすためにメインテナンスされていますが，これは永遠に続けられるわけではありません。ソフトウェアにはメインテナンスが行われているサポート期間があります。サポート期間中は定期的にセキュリティフィックスが提供されるので，これを適用しておけば，セキュリティ上の問題が発生する可能性が少なくなります。

<C>のネットカフェのパソコンは，必ずしも最新の状態に管理されているとは限りませんし，キー入力を記録してパスワードを横取りされるソフトが仕組まれていたりするので，重要な情報を扱うべきではありません。また，自分のパソコンのソフトウェアの管理は，ネットワークを接続する場所の安全性とは別の話です。

アップグレードのポイントは・・・

1	パソコンを安心して使うため，必ずアップグレードまたはアップデートを行いましょう。アップデートを怠ると個人情報が盗まれるか，データが消えてしまうかも。
2	アップデートをしていても絶対安心とはいえません。ウイルス対策ソフトなどを使って不審なソフトウェアが動いていないかチェックして，重要なデータはバックアップしましょう。

といったところです。

つばさくんは，どうすればよかったの？

OS やソフトウェアで自動更新の機能が付いている場合は，それを有効に設定しておきましょう。自動更新の機能がない場合には，ソフトウェアが提供されているところから，最新のものをダウンロードしてインストールしましょう。長く使っていない場合には手動更新が必要なことがあります。

使用しているバージョンのセキュリティフィックスなどのサポート期間が終了している場合は，最新のバージョンにするか，他の同じ機能を持ったソフトウェアに変更しましょう。

コラム１-アップグレードをしないとどうなる？-

ソフトウェアの欠陥を我慢して使わなければいけなかったり，最新の機能を使えなかったりするかもしれません。

ウイルス感染をおこしたりパソコンが乗っ取られたりしてソフトウェアがうまく動かなくなったりデータが勝手に消去されたり情報漏洩がおきたりするかもしれません。
他のパソコンへの攻撃の踏み台にされて自分が加害者になってしまうことも考えられます。

それでも過信は禁物

OSやソフトウェアを最新の状態にしておいても完全というわけではありません。不正行為を行おうとする人は，日々新しい欠陥を見つけようとし，ソフトウェアの作成者はそれを修正するというイタチゴッコになるため，セキュリティフィックスが行われるまでにどうしても時差が生じます。早ければ不具合が発覚した当日に直されるものもあれば，様々な事情で数ヵ月放置される場合もあります。もちろん誰も気が付いていない欠陥は直しようがありません。

こんな時はパソコンを買い換えましょう

OS やソフトウェアをアップデートしようとすると古いパソコンでは対応できないこともあります。その場合は残念ですがパソコンごと新しくしましょう。

パソコンを乗っ取られないために

ウイルス対策ソフトや OS のファイアウォールの機能を利用して，インストールした覚えのないソフトウェアが動いたりしていないかどうかチェックしましょう。また，いざというときのために重要なデータはこまめにバックアップをとっておきましょう。また，日頃からソフトウェアの提供者からのバージョンアップの情報に注意しましょう。

インターネットカフェの危険性

インターネットカフェのソフトウェアが最新の状態に管理されているとは限りません。すでにウイルスに感染しているか，個人情報を盗み出すソフトウェアが仕掛けられている可能性があります。

インターネットカフェで名簿作成とかネットバンキングやショッピングなど重要な情報を扱う操作はやめましょう。

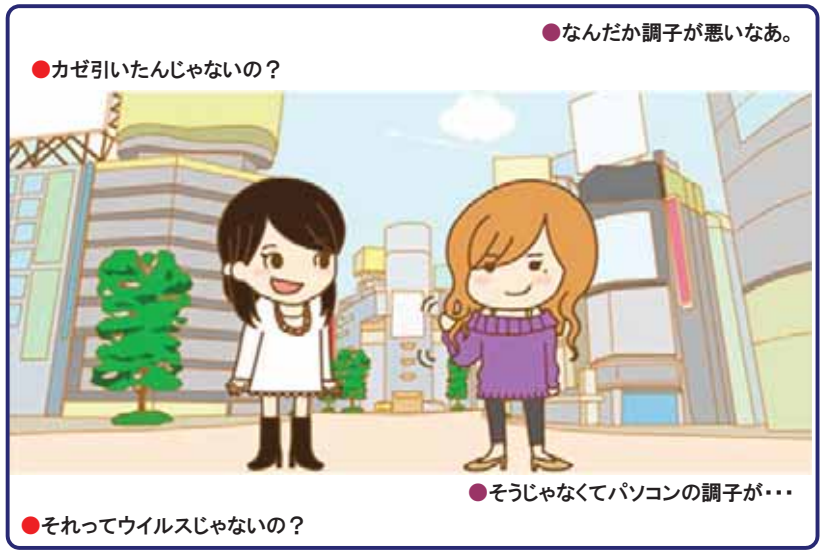
無料のソフトウェアのセキュリティのサポートは大丈夫？

オープンソースソフトウェアは C 言語や Java などのプログラミング言語で書かれたソースプログラムが入手できるので，実力のある人は，改良して使いやすくしたり，セキュリティ上の欠陥を自分で発見したり直して開発者に教えてあげることができます。世界中の開発者が協力して日々改良しているので，有料のソフトウェアよりセキュリティ上の欠陥が発見されてからセキュリティフィックスされるまでの期間が短いこともあります。ただし，古いオープンソースソフトウェアのなかには開発が終了してしまっていて，誰も保守を行っていないものもあります。2 年も 3 年も放置されているものは問題なのでウェブで最後にアップデートされた日付を確認するなど情報収集に努めましょう。

コラム２-スマートフォンのOSアップデート-

パソコンと異なりスマートフォンの OS のアップデートは携帯電話キャリアやメーカーが独自の機能の追加や機種ごとの対応を行い，十分なテストの後に提供します。このためすべての機種をサポートすることは困難で，OS 自体は最新のアップデートが発表されても古い機種はアップデートの対象から外されてしまいます。アップデートが提供されなくなったスマートフォンはセキュリティ上の欠陥が見つかっても放置されてしまいます。また，アプリケーションのアップデートの対象からも除外されることがあります。機種ごとのサポート情報に注意して早めに新しめの機種に買い換えるようにしましょう。

ウイルス対策をしましょう



第４話

対策の基本を忘れずに！

ヒカリちゃんが，風邪をひいたうえに，パソコンの調子もイマイチのようで，しずかちゃんにこぼしています。パソコンも，ウイルスに感染したのでしょう。パソコンを買ったあと，ウイルス対策しないままだったようです。パソコンのウイルスもどこにでもいて，感染の機会をうかがっています。USB メモリを使って友達とレポートを交換しただけでもウイルス感染することがあります。このようにならないためのヒカリちゃんの選択は？

さて，ここで３択問題です。考えてみてください。

【問題】　ヒカリちゃんは，本当はどうすればよかったのでしょう？	
A	ファイアウォールがあるから大丈夫。
B	パソコンにウイルスが侵入してから考える。
C	ウイルス対策ソフトを導入する。

この場合のヒカリちゃんの選ぶべき答えは

C ウイルス対策ソフトを導入する。

です。

どうして<C>なのですか？

ウイルスからパソコンを守るためには，ウイルス対策ソフトウェアがパソコンを使い始める際に導入されていることが重要です。

最近のパソコンでは，購入時にウイルス対策ソフトウェアが入っていて，使い始める時に好みのソフトを選ぶことができるのが一般的です。ただし，このようなソフトは90日間程度のお試し利用のことが多いので，お試し期間が終わる前に購入手続きをしましょう。OSの標準機能としてウイルス対策機能がついていることもあります。ウイルス対策ソフトウェアなしのパソコンをインターネットに接続して使うとウイルス感染の危険性が増大します。また，ウイルスに感染したパソコンは，ウイルスの新しい感染源となり，他の人の迷惑にもなります。

どうして<A>は間違いなのですか？

パソコンのファイアウォールは，外部からの直接的な攻撃を防ぐ機能しか持ち合わせていません。このようなファイアウォールでは，インターネットとの通信の内容まではチェックしないので，受け取ったメールがウイルス感染していても防ぐことができません。同様に見ているホームページにウイルスが仕掛けられていてもファイアウォールはチェックしません。という理由で選択肢<A>は不適切です。

どうして<B>は間違いなのですか？

感染してしまうと，貴重なファイルが消されたりパソコンの動作が不安定になりパソコンが使えなくなります。ランサムウェアといってパソコン上のデータを暗号化し，暗号化されたファイルを元に戻すのに金銭を要求するものも広まっています。ウイルスに感染すると，そのパソコンが踏み台となってウイルスの新たな感染源になったり，ボットネットに組み込まれDDoS攻撃の道具として利用されます。

ウイルス感染した場合は，パソコンからウイルスを除去して，もとのように使えるようにするより，OSも含めて再インストールすることが推奨されています。ウイルス除去にせよ，再インストールにせよ技術力とともに大変な時間と労力が必要です。なので，選択肢<B>は，最悪です。

ヒカリちゃんは，どうすればよかったの？

パソコンを使い始めると同時にウイルス対策ソフトウェアの使える機能をすべて生かすと同時にファイアウォールを有効にします。そして，これらのソフトウェアを常に最新の状態に保ちます。また，1週間に1回くらいは，ウイルス対策ソフトウェアを使ってパソコンがウイルスに感染していないかチェックします。ウイルス対策ソフトウェアの中には，「振る舞い検知機能」などの名前で未知のウイルスへの対策を行う機能をもった製品もあるので，そうした機能も有効にしておきましょう。

用語解説　「ウイルス」

ウイルスというのは，プログラムやファイルに忍ばせたプログラムで，ウイルスの仕掛けられたファイルを使ったりすると動作し，ファイルを消すとかいった悪意の活動をするものです。パソコンから情報を盗み出そうとするスパイウェアや，ファイルとは無関係

にインターネット上を動き回って感染を広げるワームというものもあります。感染すると金銭を要求するランサムウェアも話題になりました。これら悪意あるソフトウェアをまとめてマルウェア（Malware）と呼ぶこともあります。

コラム１-ウイルスのトレンド-

コンピュータウイルスには，研究レベルなら４０年以上の，日本でも３０年の歴史があります。

ウイルスとひとくくりにしても，その感染方法や被害のかたちは数年ごとに大きく変わります。これは，パソコンの利用スタイルの変化や，駆除対策の普及などに応じて，ウイルス作成者が工夫を重ねているためです。

ですので，古いウイルス対策ソフトではアップデートだけでは新しいウイルスに対応できないのが一般的です。
新しいソフトへのアップグレードをしましょう。

「ウイルス対策ソフトウェアはいつも新鮮に」

1年間に発見されるウイルスの種類は数百万にも及びます。ウイルスを使って不正にお金を得る犯罪が広まり，ウイルス作成者はより多くの人を巧妙な手口で感染させようと日々新たな工夫を重ねているためです。

これに対抗するには，新たな手口に対応できるようウイルス対策ソフトウェアを常に最新に保ち続けることが必要です。パソコン購入時に添付されていたウイルス対策ソフトウェアが有効期限を迎えたら，すぐにアップグレードや更新の手続きをするとか新しいウイルス対策ソフトウェアへ入れ替えをしましょう。

コラム２-ウイルスの被害-

大昔のコンピュータウイルスは愉快犯的なものも多く，感染すると大騒ぎになりました。

今のウイルスやスパイウェアなどは，気づかれないように感染し，気づかれないように情報を漏洩させるものや，悪意のしかけを埋め込むものが主流です。

したがって，ウイルス対策ソフトで定期的に感染しているかどうかを検査しないと危険です。

ウイルスはこっそり忍び寄る

最近のウイルスは感染してもパソコンの調子が悪くなることは少なくなりました。多くのウイルスは犯罪目的で作成されていますので，感染したパソコンのユーザに気付かれないよう，こっそり個人情報などを盗んでいきます。また，ウイルスを使えばパソコンをインターネット越しに利用できるので，あなたのパソコンが誰かに勝手に使われた結果，あなたをサイバー犯罪の犯人に仕立て上げてしまうかも知れません。

たとえ「大切な情報はパソコンに入れていない」という人でも，インターネットに接続する時にはウイルス対策を忘れてはいけません。ウイルス対策ソフトウェアをパソコンに入れないで使うというのは論外です。が，日々新しいマルウェアが生み出されているので，ウイルス対策ソフトウェアにも目こぼしがあることを理解の上で注意深くパソコンを使ってください。

フィッシング詐欺対策

第５話

「パスワードを変更して」というメール？

ケイタくんとつばさくんがバス停で話しています。ちょっと聞いてみましょう。

つばさくん宛にクレジットカード会社から電子メールが届いたようですね。メールには，セキュリティ強化のためにメール中のリンクをクリックしてパスワードを変更してくださいとあったようです。最近海外旅行からもどったばかりのつばさくんは不安になってケイタくんに相談しています。

さて，ここで３択問題です。

【問題】　つばさ君は，本当はどうすればよかったのでしょう？	
A	メールのリンクをクリックしてパスワードを変更する。
B	メールの問い合わせ先に電話して確かめてみる。
C	無視する。

この場合のつばさ君の選ぶべき答えは

C 無視する。

です。

どうして<C>なのですか？

銀行やクレジットカード会社が不正利用を検知した場合にメールで連絡することはありません。なので，そのようなメールはウソと思って間違いありません。だまされてリンクをクリックしてパスワードやカード情報を入力してしまうと，犯罪者の手に情報がわたり，ネット通販などで不正利用されます。このようなやり口をフィッシング（phishing）詐欺といいます。リンク先にマルウェアが仕込まれていてクリックするだけで感染し，機密情報を抜き取られることもあります。

相手は何かの名簿やメールアドレス集から大量に詐欺メールを送っています。返事を送るとか，クリックをすると，詐欺に引っ掛かりそうな人としてリストされます。とにかく，このような連絡は無視するにかぎります。

<A>はどのくらい危ないのですか？

犯罪者が作ったページでカード情報を入力してしまうと，その情報を使って買い物をされ請求があなたに来ます。

<B>じゃだめですか？

書いてある電話番号は多くの場合はねつ造ですが，もし犯罪者の電話につながると，こちらの電話番号が犯罪者に伝わるので危険です。架空請求の場合は，電話をするとカモとみなされて

脅されようになることもあります。もし心配で，どうしても確かめたいならば，カードの裏に書いてあるカード会社の窓口に電話するべきです。

つばさ君は，どうすればよかったの？

フィッシング詐欺や架空請求は無視することが一番です。反応したことが相手に伝わると，新たな攻撃を招きます。電子メールの差出人等の情報は簡単に偽装できるので，メール中のリンクや添付ファイルを不用意にクリックしないようにしましょう。

ウェブサービスの普及につれて，ネットオークション，オンラインショッピングや銀行，クレジット会社，支払い代行会社がフィッシング詐欺のネタに使われています。これらにアクセスする必要がある場合には，届いたメール中のリンクをクリックせずに，公式の URL を入力するか，ブックマークを使います。検索サイトの結果表示を操作して悪意のあるサイトに誘導する手口もあるので，検索結果からアクセスすることも危険です。

フィッシング詐欺を考える場合のポイントは・・・

1	カード番号の問合せは，きっと詐欺なので，無視する。
2	どうしても気になるなら，届いたメールの連絡先ではなく，カード裏面の電話番号や正式の書類にある確実な連絡先に連絡する。

といったところです。

用語解説　「フィッシング」

phishing と書きます。釣りを意味する fishing と同じ発音ですが，精巧な(sophisticated)釣りとしてこう書かれます。電子メール等で精巧なエサをまいて被害者を釣ることからきています。

コラム１-本物っぽい案内が来たらどうするか-

ネットショップの会社から，サイト移転の案内がきたらどうすべきでしょうか？

本当ならば，ホームページで案内しているはずです。それがなければ偽物と考えます。なお，ホームページを見に行くときに，メールの中のアドレスをクリックするのでなく，アドレスを直接入力するか，ブックマークを使いましょう。

重要な連絡が本物か確かめたかったら

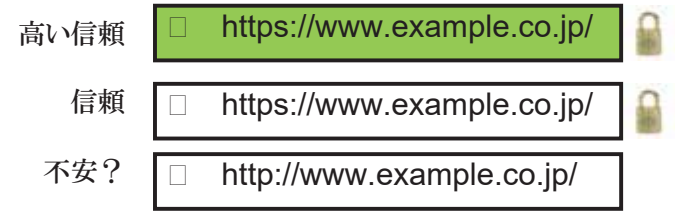
金融機関等やオンラインショッピングサイト等からのメールで偽物の確信がもてなかったら，メール記載の連絡先でなく，契約書や入会サインアップした際の記録にある連絡先に確認しましょう。最近では，スマートフォンメーカをかたった本物そっくりのメールが届くことが増えています。メールの正当性を見る目を身に着けることは大切です。

コラム２ - EV　SSL -

ネットショップやネットバンクを使うとき，アドレス欄が緑色になることがあります。これは，会社の本物のウェブサイトであることを，ふつうの鍵マークよりも高い信頼レベルの“ＥＶ　ＳＳＬ”で確認したという意味の表示です。送金など伴うサイトでは，鍵マークを必ず確認してください。

ショッピングサイトでブラウザが警告を表示したら

そのようなウェブサイトは信用できません。金銭的被害がなくても，個人情報の管理もずさんな会社かもしれません。



コラム３-セキュリティ番号-

クレジットカードにはふつう裏面に３桁のセキュリティ番号（表に４桁というカードもあります。）があります。これが知られるとカードを持っている本人の証明になってしまうので，特に注意してください。

匿名ってほんとうに匿名？

第６話

ニックネーム登録の SNS やミニブログでは本当の投稿者はわからない？

ヒカリちゃんは，最近人気の SNS（ソーシャルネットワーキングサービス）の書き込みについてしずかちゃんと話しているようです。

どうやらヒカリちゃんは，ニックネームしか表示されない SNS では何を自由に書き込んでも大丈夫と思っているようですが，本当にそうなのでしょうか？そもそも，SNS でいう匿名は本当に匿名だと思ってよいのでしょうか？

SNS にうかつな書き込みをするとトラブルに巻き込まれるもとになります。いつもの３択問題を見ながら対策を見てみましょう。

【問題】　SNS に情報を書き込むときはどうすれば良いのでしょう？	
A	匿名なのだから，言いたい事を書いても構わない
B	匿名だけど，名前を名乗って書けば，言いたい事を書いても構わない
C	SNS などで，不確かなことや不用意な事は書かない

この場合のヒカリちゃんの選ぶべき答えは

C SNS などで，不確かなことや不用意な事は書かない

です。

どうして<C>なのですか？

相手の顔を見ることなく，文字だけで意見をやりとりする SNS やミニブログでは，とかくトラブルが起こりがちです。ちょっとした言葉の行き違いや感情のもつれから，相手への罵倒や罵り合いが始まってしまい，最悪の場合はそれがもとで恐喝や傷害などの刑事事件になることがあります。SNS では炎上も日常茶飯ですので，トラブルを避けるためにも，不用意なことは書き込むべきではないのです。SNS への不用意な書き込みが原因で就職活動に失敗したとか，職を失ったという例もあります。

事実無根にも関わらずネット上に「ここのラーメン屋はまずい」とか「あの店の商品はニセ物だ」などと書き込むと，場合によっては損害賠償を求められるとか，名誉毀損で訴えられます。

どうして<A>と<B>は間違いなのですか？

そもそもネットワークにおける匿名性というものは期待できません。少なくとも，「どの端末（コンピュータ）から，いつ書き込まれたのか？」は比較的容易に調べられます。他の書き込み内容から身元が特定されることもあります。捜査機関や弁護士などが手続きを経て照会すれば ISP（プロバイダ）から発信者情報を入手することも可能です。ですので<A>は間違いです。

逆に，堂々と実名や所属を名乗ってしまったために，その情報をもとに嫌がらせに遭わないとは限りません。実際，所属の大学

やサークル，さらには顔写真などを掲示板や Web ページに載せてしまったことによってストーカ被害に遭うこともありますので，不用意にそのような情報を不特定多数の人に閲覧可能にすべきではありません。

SNS やミニブログを使う際に気をつけるべき事は・・・

1	書き込んだ個人を特定するのは容易だと認識すべし → 違法な行為や反社会的な情報を書き込まない。
2	風評被害を受けた会社から，損害賠償を請求されることもある。
3	不用意に個人を特定できる情報を載せてしまうと，ストーカや嫌がらせに遭うことがある。

といったところです。

匿名掲示板や SNS で個人を特定することが容易である理由については，この後のコラム1を参考にしてください。

「ミニブログやニックネームで参加できる SNS は，しょせん無責任な場所なのだから，何でも好きなことを書いても大丈夫だ」と考えないことです。匿名かどうかと無関係に誹謗中傷や流言飛語は犯罪です。また，面白半分で「○○駅に爆弾を仕掛けた」などと書き込むと犯罪になります。

一方，ネット上で自分の本名や，写真といった直接本人特定に使える情報だけでなく，学校名やよく利用する店といった情報も総合すると個人特定が可能で，結果として思わぬ被害に巻き込まれることがあります。世界中からその書き込みが読めてしまうことを自覚する必要があります。

コラム１-ネットの匿名性のウソ-

「ネットワークは匿名だから何を書き込んでも分からない」と思っていませんか？ 実際には，ネットワークに匿名性はほとんどありません。
法的資格を持つ者が手続きを踏めば，どこの端末から書き込んだのかは，特定することが可能なのです。

この端末情報とあわせて，入退室記録などの情報を組み合わせることによって，かなり確実に個人を特定することができます。

IP アドレスがあなたを特定する情報になるとき

インターネットにつながっているすべてのコンピュータには，「IP アドレス」という番号がついています。これは，あなたが利用している ISP が，あなたが正当な利用者であることを確認した上で割り当てているものです。詳細は第11話の「架空請求」の解説を読んでみてください。

11話では「IPアドレスや個有識別番号が知られても，業者に個人情報が伝わっているわけではない。」と解説していますが，これは相手が詐欺行為などをたくらんでいる犯罪者から見た場合です。裁判所の命令などがあれば，ISP は，あなたが使っているアドレスであることを開示します。したがって，あなたが加害者であるとみなされる場合は，あなたは相手から特定されてしまうのです。次のコラム2も参考にして下さい。

コラム２-プロバイダ責任制限法-

ネット上で権利侵害があった場合には，プロバイダ責任制限法が役に立ちます。
名誉毀損や著作権侵害等などの被害を受けた人は，プロバイダ責任制限法に基づいて，ISP（プロバイダー）に情報開示を求めることができます。

また，この法律で言う「特定電気通信役務提供者」とは，営利企業としての ISP だけでなく，フリーで運営する掲示板の管理者なども該当するので掲示板等の管理者は注意が必要です。

この法律は私たちにどのように関係するの？

プロバイダ責任制限法の役割は主に二つあります。

一つ目は，ネット上で権利侵害が行われている場合に，「特定電気通信役務提供者」（ISP）や掲示板管理者のことです）は，その情報を手続きに添って削除しても免責されるということ。この法律がプロバイダ責任法でなく，責任制限法と呼ばれているのはこのためです。この場合の権利侵害とは，著作権侵害，名誉毀損，プライバシー侵害などを言います。

二つ目は，権利侵害をなされた者は，その情報発信者の氏名・住所・メールアドレスなどの開示を ISP 側に求めることができるということ。ISP が開示を拒んだ場合は，裁判によって開示を争うことになります。

ＳＮＳとの付き合い方

第７話

別のサイトからの SNS への自動投稿は危険！

ヒカリちゃんは，SNS で失敗して，大量の迷惑メッセージをばらまいてしまったようです。

SNS で「無料占いサイト　URL をクリック」という投稿を好奇心からクリックしたら，「結果を SNS へ投稿」と出たので何も考えずに「はい」と押したら，ヒカリちゃんの ID で大量の宣伝メッセージがばらまかれました。

SNS の投稿の中のリンクのクリックには注意が必要ですね。

いつもの 3 択問題を見ながら対策を見てみましょう。

【問題】　別のサイトから SNS への投稿をクリックしたヒカリちゃんは，どうすればよかったのでしょう？	
A	おもしろそうだから「はい」を押す。
B	「投稿を許可？」と聞かれたら×をクリックして閉じる。
C	以前は問題がなかったから「はい」を押す。

この場合のヒカリちゃんの選ぶべき答えは

B 「投稿を許可？」と聞かれたら×をクリックして閉じる。

です。

どうして<B>なのですか？

「おもしろ動画」とか「モニタープレゼント」や「おもしろ占い」といったリンクつきの投稿を見かけたことはありませんか？　メッセージにリンクがあることもあります。

そのような投稿のリンクをクリックすると「結果を SNS に投稿」とか「このソフトに書き込みを許可しますか？」といった表示が出ることがあります。許可すると，本人しかできない書き込みやアプリの設定変更をソフトに対して許すことになります。許可したソフトは，あなたの ID で投稿するとか，アプリの設定も変更できます。また，プロファイルや友だちの情報等を抜き出すだけでなく新たにフォローしたりします。

実際に広告のクリックや SNS の投稿のクリックから有名サングラスの偽物販売の広告とかブランド靴の偽物の広告に大規模に悪用されたことがあります。

どうして<A>と<B>は間違いなのですか？

別サイトに SNS への投稿を許可してよいのは，複数の SNS に同時に投稿したいような場合のみです。おもしろ動画や占いとかモニタープレゼントにつられての軽い気持ちでのワンクリックから，あなたの情報だけでなく，友だちのいろいろな情報がアプリに抜き取られるというのは避けたいところです。ましてや，悪質な宣伝をあなたの名前でばらまかれたりすると信用をなくします。会社の ID だったりすると，大きな損失になります。

SNS やメッセンジャーのメッセージ中のリンクは・・・

1	あやしいサイトをクリックしない。
2	他のサイトによる投稿は許可しない。

といったところです。

SNS 間で投稿を共有したい場合以外は原則として投稿を許可しないようにします。

コラム -アプリ連携の機能-

あらたな SNS サービスの利用開始しようとすると，新しく ID を作成するというオプションの他に，別な SNS の ID でログインするというオプションが表示されることが普通です。これをアプリ連携といいます。アプリ連携では，「アクセス許可を受けた」という情報が使われます。連携が許可されると他のアプリに設定されている情報を受け取って利用者のプロファイルの設定を簡略化できるとか，サービスをまたがって記事をポストできて便利です。なので悪用されると厄介です。

アプリ連携をしてしまった場合

うっかりアプリ連携を許可してしまって，メッセージをばらまいてしまったら，まず問題のアプリのパスワードを変更します。その後，その SNS の設定画面でアプリ連携を調べて問題の連携の解除をします。

人に聞く前に自分で調べよう！

専門性が高い人も見ている SNS では，知識不足の人がうかつに書き込むと「お前はそんなことも知らないのか!?」と責められることがあります。これは，専門家の素人いじめという面もあり，ほめられたことではありません。それでも，専門家から見ると，「聞けば教えてくれるのが当然」という姿勢で質問する人があまりに多いのに辟易（へきえき）しているからとも言えます。

なんでもかんでもネット上で聞くのは良くありません。分からないことがあれば，まずは図書館などで文献を調べましょう。今はネット上に用語事典的なサイトも数多くあり，ちょっとキーワードを入れるだけで色々な知識を得ることができます。

それでもわからないことがあれば，ネット上の質問サイトで尋ねることは悪いことではありません。既出の質問でないことを確かめた上で，「調べてみて，～のようなことはわかったが，～がよくわからない」のように質問すると，丁寧に回答してくれる人はたくさんいます。ネット検索や質問サイトの特性を知ったうえで上手に使いましょう。ただし，くれぐれも宿題の答えを聞かないように！

揚げ足を取りたがるネットクレーマーに注意！

世間には，何気ない小さなことを鬼の首を取ったかのように騒ぎ立てて，事を荒立て大きくしたがる人がいます。実際，「未成年なのに飲酒をした」だとか「高校時代に煙草を吸ってみたことがある」と SNS に書いただけで，その人の所属の大学や会社を，手間をかけて調べ上げ，連絡する人がいます。たとえ，あなた個人が直接に非難・攻撃されなくても，あなたが所属する組織の誰かがこの応対に余分な労力を使うことになります。炎上したりすると，あなたや所属組織のブランドと傷つけることにもつながります。

データの受け渡しとＵＳＢメモリ

第８話

ＵＳＢメモリを無くしてしまった

いつものように，ケイタくんとつばさくんが話しています。

おや，つばさくん，北海道旅行で撮影した写真が入っていたUSB メモリを紛失してしまったようです。メモリには，北海道の雄大な風景写真だけでなく，他人に見られたら恥ずかしいつばさくんの写真も保存されていたようです。誰かに写真を見られてしまうのではと心配になったつばさくんはケイタくんに相談しています。

さて，ここでいつもの３択問題です。

【問題】　USBメモリをなくしたつばさくんは，本当はどうすればよかったのでしょう？	
A	落としても絶対見つかるような大きいメモリを使う
B	認証機能付きや暗号化機能付きのUSBメモリを使う
C	バックアップ用に同じメモリを用意する

この場合，つばさくんの選ぶ答えは

B 認証機能や暗号化機能つきのUSBメモリを使う

です。

どうして，<B>なのですか？

重要なデータは持ち出さないことが一番大事ですが，持ち出す場合には細心の注意を払いましょう。それには認証機能や暗号機能を使うことです。USB メモリには，指紋認証やパスワードを入力しないとメモリ内のデータにアクセスできないものがあります。また，内容を自動的に暗号化し，簡単な操作で復号できるものもあります。このような機能を持つ USB メモリを使うことで，万が一の紛失時にも重要なデータの漏洩を防ぐことが可能です。OS がファイルを指定して暗号化・復号機能を持つ場合には利用しましょう。

どうして，<A>と<C>は間違いなのですか？

落としても見つかるような大きな USB メモリは，持ち歩くのに不便です。紛失しないようにすることは重要ですが，それだけでは不十分です。メモリ内のデータに関単にアクセスできないようにすることが必要です。という理由で<A>は不適切です。

バックアップ用にデータを複製した USB メモリを用意すれば，USB メモリを紛失してもデータを紛失することはなくなります。しかし，紛失した USB メモリは何の対策もとっていなければ，データは見られてしまいます。データを紛失してしまうことは損害ですが，紛失した USB メモリのデータを誰かに見られてしまうことも危険です。という理由で<C>は不適切です。

つばさくんは，どうすればよかったの？

軽量コンパクトで大容量化が著しい USB メモリ等のモバイルストレージはデータの持ち運びに大変便利ですが，紛失しやすいという危険もあります。他人に見られては困るようなデータを保存し持ち運ぶ場合には，データのセキュリティ設定が可能な USB メモリでアクセス制限機能を使うべきです。データの量や秘密の程度によってはクラウドを介してデータを交換することも考えましょう。その場合には，公開範囲の設定に気をつけましょう。

ＵＳＢメモリを考える場合のポイントは・・・

1	データを持ち歩くときには，認証機能付きのUSBメモリを使う。
2	USBメモリを紛失しないように注意する。
3	記録するファイルのデータを暗号化する。

といったところです。

万が一の紛失に備えて

USB メモリのデータを安全に管理するために認証機能の付いたものや，保存するデータを暗号化するなどして，万が一 USB メモリが他人の手に渡っても，簡単に中のデータを見られないようにすることが大切です。

基本は紛失しないように

USB メモリそのものを紛失しないように，ストラップをつけたり，ケータイと一緒にしたり，紛失しないように注意することも大切です。

得体の知れないUSBメモリの危険

だれが使ったかわからない USB メモリは，絶対に使わないでください。拾ったとか家のポストに投函された USB メモリには，マルウェアが仕込まれているかもしれません。USB メモリを介して感染するウイルスが猛威を振るったことがあります。

コラム１
-普通のＵＳＢメモリを安全に使うには？-

認証機能付のＵＳＢメモリを使わずに，安全に情報を受け渡したいときはどうしたらよいのでしょう？

ファイル単位で暗号化できるなら暗号化します。また，ファイルにパスワードを設定しましょう。オフィスソフトなどでは，文書ファイルそのものにパスワードが設定できます。そうでない場合は，パスワードの設定できる圧縮ソフトで圧縮したものを保存します。このときのパスワードは文字数を長めにしてください。

認証機能付のＵＳＢメモリ

情報漏洩対策のために認証機能を備えたUSBメモリが売られています。例えば，暗証番号を入力するボタン等を備えたものや，指紋認証機能を備えたものがあります。

また，USBメモリに付属しているソフトウェアによって，USBメモリの中にパスワードで保護された領域を作成するものや，USBメモリ全体を保護する機能を持つものもあります。

個別のファイルを暗号化することが面倒だという人は，こういう機能のついたUSBメモリの利用を考えてもよいでしょう。

ネット出会い

第９話

ネットで知り合った人から「会いましょう」と連絡が来た

いつものように，ちょっと不思議ちゃん系のヒカリちゃんとしっかりもののしずかちゃんが話しているようです。聞いてみましょう。

どうやらヒカリちゃんはネットで知り合った人と会おうとしているようですね。SNSで知り合いになって，大学が発行したメールアドレスを教えてくれた相手で，寄付を頼まれている。「寄付」とはいかにも怪しそうですが･･･。

さて，3択問題です。

【問題】　会おうとしたヒカリちゃんは，どうすればよかったのでしょう？	
A	悪い人かもしれないので，完全武装していく
B	寄付を頼まれたので，借金をして持っていく
C	会う場合は，よく確かめる事。また，可能であれば，極力複数人数で会うこと

この場合，ヒカリちゃんの選ぶべき答えは

C	会う場合は，よく確かめる事。また，可能であれば，極力複数人数で会うこと

です。

どうして，<C>なのですか？

インターネット上では，実生活での人柄は隠しとおすことができますし，最悪の場合，相手は犯罪者かもしれません。ネットで親しくなったからといっても，実際の相手のことをよく知らないのですから，注意すべきです。相手が詐欺やその他の犯罪目的で近づいてきたかもしれない，と頭の片隅では考えておきましょう。一対一で会うと，相手が詐欺師の場合，冷静な判断ができなくなりがちです。暴力にも備えて，できれば複数人数で会ったほうがよいでしょう。

どうして，<A>と<B>は間違いなのですか？

悪い人かもしれないことを前提に準備するのはよいことですが，防具とヘルメットを借りてまで会いに行く必要があるかどうか，よく考えるほうが重要です。という理由で<A>は不適切です。

また，会いたい理由が寄付や借金であれば，ネットでの知り合いとはいえ，実生活で見ず知らずの人に頼むこと自体が怪しいですよね。よほど確かな情報があるのでなければ会ってはなりません。だから，<B>の選択は最悪です。

ヒカリちゃんは，どうすればよかったの？

まずは，相手のことをできるだけ調べましょう。SNS内外できちんとした情報発信や意見表明をしているかなどをよく確かめておくべきです。寄付を頼まれているのであればどのような団体がどのような寄付を募集しているのか，くらいは調べてから会うべきでした。その上で，しずかちゃんのような友達についてきてもらうのがより安全です。

ネットで出会った人と実際に外で会う場合のポイントは・・・

1	ネットで出会った人と実際に会う時は，よく確かめる事。
2	初対面の際は，できるだけ複数人で会う。
3	メールのドメインは参考になるが，偽装かもしれないので注意する。

といったところです。

少なくともネット上での情報を確かめる

SNSで知り合ったのであれば，相手が書いた日記やコメント，他の人からのコメント，など，あらためて，人となりを振り返ってみましょう。SNSの外にブログをもっているような場合には，その内容も確認したほうが良いですね。メル友であれば，メールが偽装されていないかどうか，メールのヘッダ情報で確認しましょう。

用語解説　「ヘッダ情報」

電子メールの文面の上部（ヘッダ）には，電子メールが送信されたときから受信されるまでに，送信者が指定したか，利用されたコンピュータが追加した様々な情報が記録されています。これらをヘッダ情報と言います。

電子メールソフトやウェブメールでは，from，to，cc のように，送信者が指定したヘッダ情報以外を表示していないものが多いですが，「ソースの表示」機能等により，偽装かどうかを判定するのに必要なヘッダ情報を確認することができます。

スマホの場合，これらの情報を確認できないことも多いので，より注意深く振舞ってください。

コラム１-メールの偽装-

メールの from 行は，メールソフトが設定したとおりに表示されますので，簡単にごまかすことができます。
ヘッダ情報のうち Received 行の一番下から順番に相手が使ったサーバをしらべましょう。自分の使っているメールのプロバイダや大学のサーバ受信するところまでです。相手が使っているはずの大学やプロバイダのＩＰアドレスやサーバ（ホスト）名が無ければ偽装されています。

極力，複数人数で会う

一対一で会うと，相手が詐欺師の場合，冷静な判断ができなくなりがちです。暴力にも備えて，できれば複数人数であったほうがよいでしょう。

本名や住所は簡単には教えない

飲食店や旅先で出会った人に簡単に本名や住所を教えないですよね。ネットで出会った人も同じです。ネットの外であった時も人となりが確認できるまで，本名や住所は明かさないようにしましょう。

出会い系サイトで「年下の男の子」を探す？

大学生のヒカリちゃんやしずかちゃんは，18歳以上ですから，出会い系サイトでの出会いを求めること自体は禁止されていません。しかし，出会い系サイトで18歳未満の人（「児童」）に異性交際を求める書き込みをすることは禁止されており，セックスや金品の授受を目的とした異性交際をもちかけるのは犯罪です。

コラム１２ -出会い系サイト規制法で禁止される書き込み？-

出会い系サイト規制法により，出会い系サイト事業者だけではなく，サイト利用者の行為にも刑罰が課されています。

犯罪となる書き込みは，出会い系サイトの掲示板で 18 歳未満の人（児童）を性交の相手方とする交際を求めるか児童を相手方とする金品を目的とした異性交際を求めるものです。

罰則は無いですが，児童との異性交際を求める書き込みは，性交や金品の授受をにおわせなくても禁止されています。

用語解説　「出会い系サイト」

「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」（通称「出会い系サイト規制法」）により定義されている「インターネット異性紹介事業」が出会い系サイトの法律上の正式な名前です。男女の出会いを目的としているサイトで，掲示板のように参加者にオープンな場所で異性交際を希望するメッセージが投稿でき，投稿を見た人が投稿者に対して1対1のメールやインスタントメッセージを送れる機能を備えているものに限られます。

参考サイト　警察庁　あぶない！出会い系サイト

http://www.npa.go.jp/cyber/deai/index.html

なお，出会い系サイトを通じて知り合った児童に，現金等の対価を渡して買春をすると，児童買春・児童ポルノ法違反で処罰されます。

怪しいソフトウェア，アプリ

第１０話

そのアプリは大丈夫？

いつものように，困った目にあうのはつばさくんのようです。今回はどうしたのでしょう。

いくらなんでも，何もしないで10万円もらえる話が転がっているわけはないことは，つばさくんも理解しているようですが，そのアプリの評価に，「ダウンロードして儲けた」などのおすすめがあったので信じてしまったのかもしれませんね。

さて，ここでいつもの３択問題です。

【問題】　怪しそうなソフトウェアを見つけたつばさ君は，本当はどうすればよかったのでしょう？	
A	いろいろ調べてから，インストールするかどうか決める
B	鉛筆を転がして決める
C	おすすめが出たのだから，速攻でインストールする

この場合，つばさくんの選ぶべき答えは

A いろいろ調べてから，インストールするかどうか決める

です。

どうして，<A>なのですか？

インターネットに限らず，ふつう広告というのは自分に都合のよいことしか書いてありません。使う側が，それがきちんとしたものかどうかを調べる（これを「裏を取る」といったりします）必要があります。アプリのインストールだけで儲かるというようまい話は絶対にありません。アプリが勝手に有料の電話サービスに国際電話を掛けて，アプリ製作者が利益を得るという例はありました。

怪しいと思ったらインストールしないようにしましょう。また，アプリは正規の配布サイトから入手してください。

スマートフォンのソフトウェアの場合は，公式マーケット以外で配布されているソフトウェアを絶対に入れないでください。これには例外はありません。

どうして，<B>と<C>は間違いなのですか？

「おすすめ」などの評価は，ソフトのよしあしの参考にはなりますが，サクラという場合もあるのでそれだけを信用するのは危険です。こうした理由で<C>は不適切です。

インターネットでは原則として自己責任で行動する場所だと言われます。ですので，自分で判断することを放棄している<B>の選択は最悪です。

つばさくんは，どうすればよかったの？

さきほど，「信用できるお店で買う」のがよいと説明しましたが，インターネットではどうすれば同じことになるのでしょう。まず検索サイトなどで，そのソフトについての良い情報，悪い情報を集めた上で，ダウンロードするかどうかを判断することが肝心です。詐欺などに使われるソフトは多くの場合，注意を喚起する情報が出ているはずです。また，スパイウェアなど悪質なソフトの場合は，ダウンロードしようとするとウイルス対策ソフトが警告してくれます。ただしこの場合，新しいソフトに対応するため，ウイルス対策ソフトのアップデートをしておく必要があります。

怪しいソフトウェアを考える場合のポイントは・・・

1	検索サイトなどで調べて，怪しい噂のあるソフトウェアはインストールしない。
2	パソコンには，ウイルス対策ソフトは必ず入れて，常に最新にアップデートしておく。
3	怪しいソフトウェアに関して，流行の手口などの情報を常に仕入れておく。

といったところです。

「怪しいソフトウェア」の特徴

ネットワーク上で流通している怪しいソフトウェアは，2 種類のビジネスモデルを持っています。一つは高い機能や性能を持つかのようにネット上で宣伝していますが，実際には全く役に立たないソフトウェアで，有料で販売されています。特に，「いま利用中

のソフトでは不十分なので我々のソフトに乗り換えなさい」とかという表示とともに，ダウンロードサイトを勝手に表示すると言った強引な広告には要注意です。このようなものの中には，クリックするとソフトをインストールしパソコンやスマホのデータを暗号化し金銭を要求するランサムウェアがあります。

もう一つは無料のソフトウェアとして流通しながら，個人情報を集めて流出させるもので，スパイウェアと呼ばれます。こちらは一見して通常のソフトと見分けることはなかなか難しいですが，多くの場合はウイルス対策ソフトウェアが検出して警告してくれます。

コラム１-偽ウイルス対策ソフトに注意-

ここで紹介した「怪しいソフト」で今最も多いのが，偽ウイルス対策ソフトです。

こうしたソフトは本物のウイルス対策ソフトより安く，機能は高いことを売り物にしており，インストールするとありもしないウイルスを次々と検出してあたかも高い性能を持っているかのように動きます。しかし実際には全く役に立っていないばかりか，逆にそのソフト自体がスパイウェアの機能を持っていることもあります。

Web 上の広告を使って「いまお使いのウイルス対策ソフトでは検出できないウイルスを検出しました！」といった表示とともに，強引に乗り換えを勧めてくるのが特徴です。セキュリティに関わるソフトウェアは，特によく調べてからインストールするようにしましょう。判断に迷ったらダウンロード販売に頼らず，店頭でパッケージ製品を購入するとよいでしょう。

フリーソフトの種類

フリーソフトは無料で使えるソフトウェアのことです。無料で使えるとはいえ，個人利用に限るなど使用条件がついている場合もあります。ソフトウェアをどのように作成しているかを表すプログラム（ソースコード）を一般に公開しているソフトウェアはオープンソースソフトウェアと呼ばれ，こちらも無料で使えるのが普通なので，フリーソフトの一種として扱われることがあります。フリーソフトのほか，試用してみて，有用だったら作者にお金を払うことを条件にしたシェアウェアもあります。

コラム２-フリーソフトは怪しいソフトか？-

インターネットで「フリーソフトです」と無料で提供されているソフトは怪しいものなのでしょうか？

正解は「両方ある」です。善意で作られており，広く使われているものもあれば，スパイウェアなど悪意あるソフトウェアもあります。

フリーソフトを使う場合のポイントは，ほかの人から良いと評価されているものを選び，信頼できるＷｅｂサイト，特に開発団体の公式 Web サイトからダウンロードすることです。

架空請求

第１１話

スマホに支払い請求が出た。さぁ，どうする？

いつものように，ちょっと不思議ちゃん系のヒカリちゃんとしっかりもののしずかちゃんが話しているようです。聞いてみましょう。

どうやらヒカリちゃんのスマホに 3 万円請求するぞ，という表示が出たようです。そのとき，スマホの個有識別番号とか IP アドレスとかが知られているようだったので大慌て。

さて，ここでいつもの3択問題です。

【問題】　請求画面を見たヒカリちゃんは，これからどうすればよいでしょう？	
A	遅れないように請求された金額を送金する
B	断固無視する
C	「そのサイトは見た事がない」と先方にメールを送る

この場合，ヒカリちゃんの選ぶべき答えは

B 断固無視する

です。

どうして，<B>なのですか？

ヒカリちゃんが，業者から取引の条件を知らされた上で，自分の意思でサービスに申し込んだり，データを買ったりした結果，請求されたのであれば，支払う義務があります。しかし，ネットを閲覧していて，サービスやデータの販売条件や確認画面が表示されないうちにリンクをクリックしたり，ボタンを押したりしただけでは，契約を申し込んだことにはならないので，支払う理由も義務もありません。支払う義務が無い人に代金を請求する「架空請求」は，無視できますし，詐欺を目的とした悪徳業者に問い合わせをしたりするとさらに対応を難しくするので，断固として無視すべきなのです。

この対応はスマートフォンの場合でも同じです。

どうして，<A>と<C>は間違いなのですか？

支払う理由が無いのに支払ってしまっては，業者の思うつぼですよね。架空請求のワンクリック詐欺にひっかかったことになります。振り込んでしまった後で，悪徳業者にだまし取られたお金を取り戻すのは至難の技です。しかも，氏名や住所を知られることになり，一回では済まないかもしれません。入会金はもらったけど月額会費を 2 カ月分よこせ，と脅されたり，別な架空請求をしかけられたりする「カモ」扱いされたり，さらに同業者間でカモリストが情報交換されることもあります。したがって，<A>は最悪です。

また，すぐに支払いをしないとしても，無視せず，脅し文句に反応してメールや郵便で苦情を言ったり，問い合わせをしたりすれば，やはり悪徳業者の思うつぼです。連絡先を知られることになりますから，嘘の法律を説明するとともに，裁判所に訴えるぞ，警察に告訴するぞ，などの脅し文句が入った悪質な督促がメールや郵便で繰り返されることになり，さらに対応が難しくなりますので<C>の選択も不適切です。

ヒカリちゃんは，どうすればよかったの？

インターネットを閲覧しているとき，他のサイトに誘導する文面はよく確認してからリンク先をクリックしましょう。（宣伝メールからの誘導も同じです。）また，リンク先サイトに行ってしまった後，動画再生などのボタンをクリックすると，再生前に小さな文字や見えにくい文字で販売条件が書いてあることもあります。見え難い場合は契約が成立しませんので支払い義務はありませんが，見えやすい場合は，法的にも支払いする義務が発生する場合があるので，そのような場合は，絶対にクリックを続けてはいけません。

画面で支払い請求された場合のポイントは・・・

1	IPアドレスや個有識別番号が知られても，業者に個人情報が伝わっているわけではない。
2	代金や支払い期限など契約条件が表示されていなかったり，見えにくかったりしたために，無料と考えたり，なんとなくクリックしたのであれば支払う義務がない。
3	ワンクリック詐欺の他にも，メールや，ウイルスによる架空請求もあるので最新の手口を理解しておく。

といったところです。

ＩＰアドレス・個有識別番号が知られても慌てない

インターネット閲覧用のブラウザソフトウェアは，パソコンに割り当てられたIPアドレスやパソコンの名前を閲覧先のウェブサイトのコンピュータとやりとりしながらウェブサイト側が出す画面を表示します。しかし，メールアドレスやその他の情報までウェブサイトと交換することはありません。

もし，サイトを見ただけのはずなのに，メールが来るようなことがあるときはPCやスマホのセキュリティ対策に問題があります。サイトの閲覧でPC内の情報を探ってサイト運営者に送付するスパイウェアが入っているか，クレジット番号，ID，パスワードなどをタイピングした情報を記録して送信するキーロガーと呼ばれる機能をもったウイルスに感染したおそれがあります。

この場合は，ワンクリック詐欺以外の重大被害にもあうおそれがありますので，最新の情報でウイルスの検査や駆除をした上で，パスワードの変更，場合によってはクレジットカードの停止・再発行を緊急に行う必要があります。これと同じように，携帯ウェブサイトで，通知したはずの無い個人情報が表示される場合は，以前，登録した個人情報が漏えいしている恐れがありますので，場合によっては，携帯電話を変更することも考えましょう。

コラム１
-「個有識別番号」から個人情報は伝わらない-

ワンクリック詐欺業者は，ＩＰアドレスやＰＣの名前，プロバイダ情報を個有（または固有）識別番号と呼びます。ＩＰアドレスやＰＣの名前は，もともとＰＣとウェブサイトがやり取りしているもので，メールアドレスやプロバイダに登録した住所氏名等の個人情報は伝わりません。

コラム２ -ワンクリック詐欺の落とし穴-

会員登録料や動画・サービスの料金，支払期限等の重要な契約条件は，購入前に必ず表示されることになっています。

ワンクリック詐欺サイトは，動画をクリックさせる前に，小さい文字や背景色とかわらない見にくい文字で契約条件を表示するので，つい見逃してクリックしてしまいます。

クリックした結果，「個有識別番号」が表示され，覚えのない契約条件なのに料金を架空請求される詐欺なのです。

身に覚えがない架空請求は支払う義務がない

ワンクリック詐欺業者は，IPアドレスや固有識別番号，PC名，さらにはIPアドレスを管理するプロバイダ名を画面に表示し，いかにも契約が成立したかのような文言と同時に表示することによって，サービスやデータを購入する契約してしまった，姓名等の他の個人情報まで知られている，と錯覚させることを狙っています。

しかし，販売条件や，購入前の確認画面が表示される前にリンクをクリックしたり，ボタンを押したりしただけでは，購入を申し込んだことにはならないので，支払う理由も義務もありません。

支払う義務が無い人に代金を請求する「架空請求」は，無視できるので慌てずに行動しましょう。

購入申込みにあたるかも，と不安な場合には，総務省電気通信消費者相談センター，消費生活センター，警察などに相談しましょう。

架空請求の最新の手口を知っておく

ネットを利用した架空請求は，ウェブサイトでのワンクリック詐欺の他にも，PCや携帯電話の電子メールに記載されたリンクにアクセスして自動登録させるもの，携帯電話番号宛のショートメッセージサービスを利用するもの，ウェブサイトで配布されたウイルスによるものが知られています。

下記サイトでは最新の手口や対策，相談先の情報が紹介されていますので見て理解しておくようにしましょう。

国民生活センター　あわてないで!!　クリックしただけで，いきなり料金請求する手口
http://www.kokusen.go.jp/news/click.html

警察庁　インターネット安全・安心相談
http://www.npa.go.jp/cybersafety/

警視庁　よく寄せられる相談事例
http://www.keishicho.metro.tokyo.jp/sodan/nettrouble/jirei/index.html

著作権

第１２話

ウェブページ等を作るときに気をつけることは？

面白そうなことには何でもやりたがるつばさ君，今度は人気アーチスト「ノゾミーズ」を応援するための Web ページを作ろうとしているみたいです。

どうやら，つばさ君はその Web ページでノゾミーズの曲やビデオが流れるようにしたいみたいですね。

でも，ちょっと待って下さい。勝手にそんなことして大丈夫なのでしょうか？

いつものように，3択で見ていきましょう。

【問題】　ファンサイトを作ろうとしたつばさ君は，本当はどうすればよかったのでしょう？	
A	非営利のファンサイトなのでコンテンツを使ってもいい
B	ノゾミーズのファンクラブに許可を取る
C	すべての権利関係者から使用許諾を得る

この場合，つばさくんの選ぶ答えは

C	すべての権利関係者から使用許諾を得る

です。

どうして，<C>なのですか？

「著作物」は，原則として著作権者の許可なしには勝手に使うことはできないと思って下さい。ミュージシャンのプロモーション・ビデオ一本の中にも，作曲家，作詞家，歌手や演奏者（実演家と言います），そしてビデオを収録・放送した映像会社や放送局などのさまざまな人達の著作権（著作隣接権を含む）が絡んできます。ですので，もしあなたがWebでコンテンツを公開しようと思えば，すべての関係者から許諾を得る必要があります。もちろんその為には，様々な手続きが必要でしょうし，その為の費用もかかります。許可無くこのような行為を行えば著作権侵害となり，場合によっては権利者から訴えられ，刑事罰を科されることもあります。

どうして，<A>と<B>は間違いなのですか？

著作物を使用する際に著作権者の許諾が不要な場合は，著作権法の 30 条以降に定められた，ごく限られた場合だけです。具体的には，家庭内などで利用する際の複製や，大学や学校の教員が授業の教材として一部を複製する場合，また学術論文などでルールに則って引用する場合などです。 また，営利か非営利かということも著作物の使用とは直接関係ありません。非営利目的であれば自由に使える訳ではないので，これも注意が必要です。

また著作権は通常，相続や譲渡や売買をしないかぎり制作者本人に属します。ファンの集まりであるファンクラブが持っているわけではありませんよね。歌謡曲の場合は，JASRAC（日本音楽著作権協会）によって一括管理されているものがほとんどなので，一層の注意が必要です。

著作権問題のポイントは・・・

1	誰かが作った楽曲や映像など，あらゆるコンテンツには著作権があることを心がける。
2	もし使用するのであれば，予め関係者の許諾を取ることを心がける。

といったことです。

つばさ君は，どうすればよかったの？

著作権は誰がつくったものにでもある，という大原則をよく知っておくべきでした。著作物とは「思想又は感情を創作的に表現したものであつて，文芸，学術，美術又は音楽の範囲に属するものをいう。」と定められています。この定義を満たすもの，つまり単なる数字や事実などを除く，およそ人が創作したものの多くに著作権があると言えるでしょう。

また著作権は，その創作のレベルが高度である必要はありません（つまり高い芸術性を持っている必要はない）。名の通った芸術家でなくとも，皆さんそれぞれが作った楽曲や，書いた絵画・詩歌などにも当然に著作権は発生します。アマチュアの友人の撮った写真だからといって無断で使ってはいけません。

つまり，インディーズレーベル所属でまだブレイクしていないバンドの曲はもちろんのこと，たとえ趣味で演奏や作曲を行っているアマチュアバンドの楽曲であっても，著作権は当然に発生しています。

コラム１ -著作権-

著作権の英訳は〝copyright〟ですが，意味合い的には〝author's right〟と言ったほうが良いでしょう。

すべての権利保持者は作者であって，ユーザは（家庭内複製などのごく限られた場合を除いて）原則として許可を得ないと他人の著作物を使ってはいけません。

特に，ネットで勝手に公開することは，著作権のなかの複製権や公衆送信権などを侵害することになりますから，行わないようにしましょう。

著作権はさまざまな権利の集まり

「著作権」は，複製権，上演権・演奏権，上映権，公衆送信権，口述権，展示権，頒布権，譲渡権，貸与権，翻訳権・翻案権などといった様々な支分権の集合体です。また「著作者人格権」としての公表権，氏名表示権，同一性保持権があります。さらに，実演家やレコード製作者，放送事業者などは，著作者に準ずる地位にあるものとして「著作隣接権」を保持しています。例えば公衆送信権はネットワークの普及に伴って制定された権利で，ネット上で他人の著作物を公開しようと思ったら，まずこの公衆送信権の許諾を権利者から得る必要があります。もちろん著作物の種類・性質によっては同時に複製権の許諾や，レコード会社，放送局などからも様々な著作隣接権の許諾が必要になるでしょう。自分の作品以外は許可なくWebに載せない，というのが大原則です。

海賊版はアップロードだけではなく，ダウンロードも刑罰の対象

2012 年（平成24年）に著作権法が改正されて，著作権を侵害する著作物を自己のパソコンやスマホにダウンロードした場合にも，状況によっては刑罰が科されることになりました。一般には「違法ダウンロードの刑罰化」と言われるものです。この改正では，違法に複製・配信された有償著作物だと知りつつ録音・録画した場合は，たとえ私的使用目的であっても刑罰を伴う違法な複製と行為とされました。最大で2年以下の懲役もしくは 200 万円以下の罰金，またはその両方が科されます。有償著作物とは，CD/DVD として一般に発売されているもの，有料でインターネット配信されている音楽・映像等，通常はお金を出さないと購入できないようなものを言います。ダウンロード（複製）をその対象としていますので，YouTube のようなストリーミング配信を見ることは対象ではありません。詳細は，文化庁のサイトに法改正に関する解説がありますので，『違法ダウンロードの刑事罰化についての Q＆A』で検索してみて下さい。

著作権の保護期間

著作権は通常，著作者の死後 50 年で消滅します。法人の場合は，公表後 50 年間と定められています。しかし，この保護期間もその著作物が，創作・公表された時期によって保護期間が前後しますので，過去 100 年位前までのものは使用の前によく調べる必要があります。実際，「映画の著作物」に関しては 2004 年（平成 16 年）に公表後 70 年間に変更されました。また，この保護期間は今後さらに長くなることが予想され，現在延長について国内外で議論されています。結局，安心して使えるのは，数百年以上前に作られたクラッシック音楽などに限られると考えればよいでしょう。

コラム２ -肖像権-

著作権と混乱しやすい権利に肖像権があります。こちらは人格権に基づく権利で，誰もが持っているものです。

ですから，友人の顔写真なども勝手にウェブなどで公開してはいけません。自分が撮った写真だからといって勝手にウェブ等で公開すると，肖像権侵害になりかねません。

芸能人などの著名人は，肖像権とは別に，顧客吸引力に基づくパブリシティ権が認められるので，特に配慮が必要です。

ウェブページや SNS にコンテンツを載せる時の注意事項

自分が撮った写真でも，他人の顔がアップで映っていれば要注意。会場の雰囲気などを伝えたいときは，顔が判別できないよう引いて撮った写真を使いましょう。芸能人やスポーツ選手を写した写真は，たとえ自分で撮ったものでもウェブページなどに安易に貼らないようにしましょう。

メールの添付ファイル

第１３話

電子メールに添付して写真を送りたいのに

ヒカリちゃんとしずかちゃんはいっしょに旅行してきたようです。写真担当は，ヒカリちゃんだったようで，よほど楽しかったらしく，最新のデジカメで1000 枚近くも写真をとってきた様子。その写真をしずかちゃんに電子メールで送ろうと苦戦したようです。一枚10メガバイトで千枚ですか。ちょっと無理なことをヒカリちゃんは，やろうとしていたようですね。

さて，ここでいつもの 3 択問題です。

【問題】　写真をメール送ろうとしたヒカリちゃんは，本当はどうすればよかったのでしょう？	
A	クラウドドライブに置いて URL をテキストとしてメール中に書く。
B	メールが送れるまで何度でも送りなおす。
C	1枚1枚順番に 1000 回メールする。

この場合のヒカリちゃんの選ぶべき答えは

A	クラウドドライブに置いて URL をテキストとしてメール中に書く。

です。

どうして<A>なのですか？

一枚 10 メガバイトの写真が千枚だと 10 ギガバイトの容量になります。このサイズでは CD や BD に入りません。受信側のメールサーバのメールボックスに容量制限があると入りきらなくて受信できない（=メールが送れない）ということになります。メール 1 通あたり 100MB 程度までに制限しているところが多いようです。彼女のメールは，この制限をはるかに越えます。メールボックスに容量制限がなくても，回線速度によっては送信に異常に時間がかかることがあります。なにより添付ファイルはウイルス感染の原因にもなっていて，開いてもらえる可能性が低くなっています。この場合，クラウド上のファイル共有サービスが便利です。しかし，クリックで開ける形式のメールもフィッシングやマルウェア配布に使われていて，リンクを直接メールに貼るのも問題です。ここでは URL の情報をテキストとして送るのが良いでしょう。DVD に入るなら DVD で渡す方が確実かもしれないですね。

どうして<B>は間違いなのですか？

ふつうパソコンから送ったメールは，いったん送信側のメールサーバに一時的に蓄えられた後，相手のメールサーバに転送されます。このサーバで容量制限にかかったとすると，メールを繰り返し送ろうとしてもサーバに受け付けられず無駄な努力と回線を占有することになります。容量制限がなかった場合でも，しずかちゃんのメールボックスの空きが少なくなっている。とすると，ヒカリちゃんのメールはメールサーバに蓄えられたあと，しずかちゃんにメールを届けようとして，メールの再送を繰り返します。

このような行為は，悪意がなくても，メールを送られるメールサーバにとってはメールを使った嫌がらせにも見えかねません。というわけで<B>は不正解というだけでなく最悪の対処です。

どうして<C>は間違いなのですか？

容量的には一括送りと同様にメールサーバに負荷をかけます。なにより手間がもったいないですね。

ヒカリちゃんは，どうすればよかったの？

しずかちゃんの教えてくれたように，インターネット上のファイル一時預かりサイトや写真共有サービスを利用するのがよいでしょう。しかし，10GB となると，共有サイトにデータをコピーする時間も回線速度によっては問題になるかもしれません。このケースでは，原始的方法に見えますが，モバイルディスクにコピーして手渡すか郵送するのも，よさそうですね。

電子メールにファイル添付を考える場合のポイントは・・・

1	メールの添付は使わない。
2	大量のデータ転送に関しては手渡しするとか，ファイル一時預かりサイトなどを適宜使用する。
3	ファイル一時預かりといったクラウドサービスの利用にあたって，リンクを渡す方法に注意をする。

といったところです。

メールにはウイルスも添付できる

添付ファイル付きの電子メールは，ウイルス等のばらまきや特定の個人・グループを狙ったフィッシングに利用されるようになっています。たとえば，上司や指導教員の名前を使ってオフィスソフトの書類に見せかけたウイルスを送りつけるといった事例があります。相手によっては，セキュリティ上の理由から添付ファイルを許さないこともあります。

メールの添付は避けたほうが無難

なので，電子メールにファイル添付という使い方は，よほど緊急でないかぎりはやめましょう。やむを得ず添付ファイルで送る場合には，細心の注意を払ってください。

用語解説　「ギガバイト」

バイトは情報量の単位です。1 バイトは英語のアルファベット 1 文字相当です。メガは 10^6，ギガは 10^9，ちなみにテラは 10^{12}を示す補助単位です。

コラム１-メール送信の常識-

必要があって添付メールを送る場合でも実行ファイル（プログラム）の添付は絶対にやめましょう。メールプログラムによってはセキュリティ機能のために相手は添付内容を見ることができないことがあります。相手が添付のプログラムを保存することや，実行可能とするようにメールプログラムの設定を変更することは，メールプログラムのセキュリティ機能をわざわざ低く設定することになり相手はウイルスに感染しやすくなります。

添付ファイルはすぐに開かない

ファイルの添付されたメールや HTML 形式メールが送られてきても，差出人情報を鵜呑みにして，すぐにメールや添付ファイルを開くことは危険です。From は詐称できます。友達のパソコンがウイルス感染していて，ウイルスが友達の名前でウイルスを送ってくることもあります。

ウイルス検査をしてから開く

添付ファイルは，必ずウイルス対策ソフトウェアで検査してから開くようにします。怪しいなと思ったら，手持ちのソフトウェアだけでなく，オンラインのウイルス検査ポータルでも検査するといいでしょう。

コラム２
-添付メールやHTML形式メールを受信したら-

差出人を無条件に信頼して，添付ファイルを開かないようにしましょう。まず，ウイルス対策プログラムでスキャンしてください。HTML 形式やリッチテキスト形式のメールは，余計なスクリプト等が実行されないようにしてから表示してください。

HTML 形式やリッチテキスト形式のメールのあつかい

HTML 形式のメールは，ウエブのページのように，文字の大きさや色を自由に変更できたり，写真や図を見せたり，スクリプトで内容をコントロールできて便利です。

しかし，なんでもできる HTML 形式やリッチテキスト形式の機能を悪用してウイルスのばらまきも行われますので，細心の注意をはらってください。

Free Wi-Fi は危ない？

第１４話

Free Wi-Fi は危険がいっぱい？

駅前のハンバーガーショップでいつものように，ちょっとおおざっぱ系のつばさ君と，きっちり系のケイタ君が話しているようです。聞いてみましょう。

どうやら 2 人は旅行の相談をするために駅前のハンバーガーショップへやって来たようですね。ここなら Free Wi-Fi が使えて検索や予約までできて便利だというのですが，本当に大丈夫なのでしょうか？

さて，ここでいつもの 3 択問題です。

【問題】　Free Wi-Fi を利用するつばさ君は，本当はどうすればよかったのでしょう？	
A	まわりに人がいないか，確かめてから使うと良い。
B	有名なショップの Free Wi-Fi だったら，使っても 大丈夫。
C	Free Wi-Fi では情報検索程度。暗号化されていない予約サイトは利用しない。

この場合のつばさ君の選ぶべき答えは

C	Free Wi-Fi では情報検索程度。暗号化されていない予約サイトは利用しない。

です。

どうして<C>なのですか？

Free Wi-Fi のように電波を使った通信は他人も傍受できるので，利用するときは注意が必要です。閲覧しているウェブページや送受したメールを盗み見されるだけでなく，パスワードや，予約サイトで入力するクレジットカード番号や会員番号を知られて悪用される恐れもあります。暗号化された通信をしていなければ，一般的な情報閲覧に留め，メールの送受信，パスワードやカード番号，その他個人情報の入力は避けましょう。

どうして<A>は間違いなのですか？

まわりに人がいなくても，電波を使った通信は傍受されることがあります。Free Wi-Fi で使う電波は強いものではありませんが，数百メートル先まで届くことがあるし，薄い壁なら隣の部屋にも伝わってしまいます。

どうして<B>は間違いなのですか？

ハンバーガーショップが有名ブランドでも，ぜんぜん関係ありません。Free Wi-Fi を使うときに，盗聴されないように心掛けるか，確実に暗号化して使うのは，利用者の責任です。

つばさ君は，どうすればよかったの？

家庭や学校では気を抜いてよいわけでは決してありませんが，公共の場でのインターネットの利用においては一段と高いセキュリティ意識が必要です。Free Wi-Fi を安全かつ便利に使いたければ，インターネットの仕組みについて日頃から勉強しておきましょう。

Free Wi-Fi を利用する際のポイントは・・・

1	Free Wi-Fi を利用する際は，最低限，パソコン上でファイアウォールなどのセキュリティ設定をしておくこと
2	その上で，常に盗聴されている可能性を意識して，暗号化されていないサイトの利用では大事な情報の送信を控えること

といったところです。

電波を使った通信は暗号化しないと周りから見られる！

Free Wi-Fi は無線LANの技術を公共の場所での利用に応用したものです。無線LANの「LAN」はローカルエリアネットワーク(Local Area Network)の略で，「ローカル」すなわち家庭やオフィス内での利用を想定して設計されています。Free Wi-Fi は，専用の装置が不要でノートパソコンの内蔵ワイヤレスなどの機能がそのまま使える点で利便性は高いのですが，セキュリティに関しては弱く，利用にあたっては注意が必要です。

まず，Free Wi-Fi につないだとたん，同じアクセスポイントにつながっている他の端末とは「同じLAN」につながっていることになります。たとえばファイル共有の設定を家庭で使う状態のまま

にしていると，大事なファイルを見られたり書き換えられたりしてしまう恐れがあります。また，パソコンのOSのアップデートをさぼっていたりしてセキュリティホールがあると，たちまち侵入されるかもしれません。したがって，不正な侵入を受けないためには，パソコンのファイアウォールの設定を公共の場所での利用に合わせたものにしておくなどの対策が最低限必要です。パソコンのOSやウイルス対策ソフトウェアのアップデートを怠ってはならないことは言うまでもありません。

次に，無線LANが電波を利用して通信を行っていることに対する注意が必要です。暗号化されていない通信は，誰にでも見える状態でやりとりされています。あなたがどんなウェブページを閲覧しているかだけではありません。暗号化機能のないメール閲覧ソフトでメールを送受したら，そのときのメールの中身だけでなくアクセスに使っている大事なパスワードまで盗まれるかもしれません。オンラインショッピングではクレジットカードの番号を盗まれて悪用される恐れもあります。したがって，通信が正しく暗号化されていることと，通信している相手のサイトが本物であることを確認できない限り，Free Wi-Fi での通信はすべきでないのです。「暗号化されているかどうかなんて難しいことはよくわからない」という方は，ウェブでの一般的な情報閲覧に留め，メールの送受や，パスワードやカード番号，その他個人情報の入力を要するウェブページの閲覧は控えましょう。

電波は思わぬところまで伝わる！

無線LANは，特定小電力と呼ばれる免許不要の弱い電波を使っています。使われている周波数は 2.4GHz 帯で電子レンジなど他の電気機器の影響を受けやすいものです。最近では

5GHz 帯が使われることもありますが，2.4GHz 帯より直進性が強く壁などの影響を受けやすいです。家庭で無線LANを使っていて，隣の部屋にはなかなか届かなくて苦労した経験がある方もいるでしょう。「まわりにあやしそうな人は誰もいないから大丈夫」と思ってしまうかもしれません。

しかし，弱い電波と言っても，実は条件さえよければ何百メートルも届くのです。決して，見えている範囲だけではありません。薄い壁なら難なく通過しますし，壁や床で反射して回り込んだりします。また，近くにいるのが知人だからと言って油断してはいけません。その人のパソコンがウイルスに感染していて悪意のある人に乗っ取られている可能性だってあるのです。

Free Wi-Fi サービスは暗号化してくれているの？

Free Wi-Fi は，無線LANの仕組みをそのまま使っています。これは大手の通信事業者が提供しているサービスでも同じです。Free Wi-Fi サービスでは，まったく暗号化しない状態で通信を行っていることが少なくありません。スマートフォンで警告が出るような無線 LAN での通信には注意が必要です。暗号化されているサービスを使う場合は WPA2-PSK(AES)を選びましょう。この方式では，接続のたびにキーを元にして暗号化の鍵が作られるので，第三者が電波を傍受して暗号を解読するのは比較的困難です。ただし，Free Wi-Fi では暗号化のためのパスフレーズが公開されており，後述のように悪意のある第三者が偽のアクセスポイントを設置して通信を覗き見ることができるので，無線 LAN での通信が暗号化されているからといって安心はできません。

Free Wi-Fi のサービスで暗号化されていない場合には暗号化

通信にはSSLなど上位のプロトコルで行う必要があります。

外出先でネットワークを使うときのポイント

Free Wi-Fiに限らず外出先でネットワークを使う際には，パソコンのセキュリティ対策をしっかりすることが必要です。OSやウイルス対策ソフトによる対策に加え，自宅などで使っているファイル共有などを停止させます。多くのパソコンにはファイアウォールという機能が備わっており，適切な設定をすることでファイル共有などがされなくなります。

次に，悪意のある者による盗聴のリスクを考えて，個人情報やパスワード，カード番号の入力の際には細心の注意を払うことが必要です。具体的には，メールソフトウェアの設定において暗号化を使うようにしているかの確認，ウェブサイトへのアクセスの際にSSL/TLSと呼ばれる暗号化された通信モードになっているかを確認することです。また，ブラウザが「このサイトの証明書は信用できません」などの警告を出したら，暗号化はされているが偽サイトに接続させられている可能性があることを示しています。

用語解説　「ＳＳＬ」

SSL（Secure Socket Layer）は，インターネット上の通信を安全に行うためのプロトコルです。TCPなどのトランスポート層のプロトコルと，HTTP (Hyper Text Protocol)などアプリケーション層のプロトコルの間で動作します。SSLはもともとNetscape社が開発したプロトコルで，それを改良したTLS (Transport Layer Security)が標準化されていますが，それらを総称してSSLと呼ぶことがあります。ウェブのアクセスに用いられるHTTP

だけでなく電子メールに用いられるＰＯＰ (Post Office Protocol)などで広く用いられています。SSLには，暗号化の機能だけでなく，PKI（公開鍵認証基盤）を用いて通信相手を認証する機能があります。ウェブサイトは，信頼される認証局からSSLサーバ証明書の発行を受けてウェブサーバに組み込むことで，そのサイトにアクセスする利用者にサイトの真正性を確認させることができます。

研究室や自宅での無線ＬＡＮのセキュリティ

研究室や自宅で無線LANを設置する際には，セキュリティ面で改良されたWPA2-PSK(AES)や認証機能のあるWPA2-Enterpriseと呼ばれる方式を用いましょう。

無線LANと通信の傍受

誰でも傍受できてしまう無線LANですが，以下のような行為は電波法で禁止されています。

・特定の相手方に対して行われる無線通信を傍受してその存在若しくは内容を漏らし，又はこれを窃用すること（第59条）

・暗号通信を傍受した者が，当該暗号通信の秘密を漏らし，又は窃用する目的で，その内容を復元すること。（第109条の2）

「窃用」とは難しい言葉ですが，受信した内容を自分や他人の利益のために利用することです。暗号化されていない通信については，傍受するだけなら違法ではありませんが，通信の内容を誰かに漏らしたり，知った内容でなにか行動を起こしたら違法

です。仮にあなたがつばさくんの彼女の友達で，つばさくんが週末に彼女に内緒で行く合コンの連絡を偶然傍受してしまったとしても，決して彼女に伝えてはいけないのです。

なお暗号化されている通信は，暗号を解読したり解読を試みるだけで違法です（未遂罪も処罰されます）。ネット上では無線LANの解読ツールが出回っていますが，くれぐれも興味本位で試したりしないでください。

偽アクセスポイントに接続させられないように

前述のように Free Wi-Fi には盗聴のリスクがありますが，もうひとつ気をつけないといけないのは，偽アクセスポイントに接続させられるリスクです。無線LANでは ESSID と呼ばれる識別子を使ってサービスを識別しており，Free Wi-Fi でもそれがそのまま使われています。しかし ESSID は市販の無線 LAN アクセスポイントを使ってだれでも自由に設定できるので，大手の通信事業者のサービスと同じ ESSID のアクセスポイントを，悪意のある者が勝手に立てることができてしまいます。WPA2-PSK(AES)による暗号化がされていても，パスフレーズが公開されているので防ぐことはできません。偽のアクセスポイントでは，盗聴ができるだけでなく，接続してきた人のアクセスを偽のサイトへと誘導することで，パスワードやカード情報のような重要な情報を盗むことができてしまいます。SSL を使ったウェブアクセスでは，ブラウザに表示される URL，SSL を使っていることを表示する鍵のマーク，SSL で不正なサイトに接続させられたときに出る警告，以上のすべてに注意していれば偽サイトであることに気づくはずです。しかしながら，そのようなサイトを運営する

悪意のある者は，サイトを巧妙に偽装していますので，実際に見破るのは容易でないかもしれません。重要な情報の入力の際は慎重にしてください。

なお，ここで述べた危険性は Free Wi-Fi サービスに限りません。外出先でネットワークを借りてつながせてもらう場合にも同様です。有線のネットワークであっても，途中で盗聴されている可能性は否定できません。

VPNを使おう

VPN（仮想プライベートネットワーク）は，外出先から大学のサーバへ接続し，論理的には大学のネットワークに直接つながっているのと等価なネットワーク環境を実現する仕組みです。大学のネットワークで VPN サービスが提供されているか，ネットワークの相談窓口にきいてみましょう。

ネットカフェはもっと危ない

いわゆるネットカフェには，ウェブブラウズが可能なパソコンが置いてあります。これは便利に思いますが，不特定多数が利用するため，ウイルスやキーロガーなどの不正なソフトウェアが仕掛けられている恐れもあり，セキュリティ上のリスクは Free Wi-Fi よりもさらに高いです。

パスワードの管理

第１５話

ミニブログのパスワードを忘れてしまった！？

夜の街を歩きながら，ヒカリちゃんがしずかちゃんに相談しています。どうやらヒカリちゃんは，この前，複数あるミニブログのアカウントのひとつを忘れて困っているようです。それで，覚えやすい“12345678”にしようと言ったら，しずかちゃんに止められました。

それでは，パスワードはどう設定すれば良いのでしょうか？

さて，ここでいつもの３択問題です。

【問題】　パスワードを設定するときに，ヒカリちゃんは，どうすればよいのでしょう？	
A	自分が覚えやすい簡単なパスワードを設定しておく
B	パスワードを思い出すヒントをメモして，他人に見られない様に保存しておく
C	パスワードを他のサービスと共通にして，忘れてもいいようにパソコンに張っておく

この場合のヒカリちゃんの選ぶべき答えは

B	パスワードを思い出すヒントをメモして，他人に見られない様に保存しておく

です。

どうして<B>なのですか？

SNS やネットショッピング等を使うときに，パスワードで本人確認をします。パスワードを誰かに知られてしまうと，あなたに成りすまして書き込みされたり，買い物をされたりするかもしれません。なので，パスワードは絶対に知られないようにしなければなりません。パスワードを思い出せるような自分だけのヒントをメモしておいて，それを秘密の場所に隠しておけばよいでしょう。

どうして<A>と<C>は間違いなのですか？

パスワードに誕生日や電話番号，バイクのナンバーなどを使うと，覚えやすいですね。でも，あなたの友達ならばそういう情報を知っている人もいるし，パスワードを推測できるかもしれません。知らない人でもちょっと調べればそういう情報がわかるかもしれないし，そうするとパスワードを見破られて，いつの間にかネットショッピングをされたり，あなたのメールを読まれたり，ブログに書き込まれたりするかもしれません。という理由で<A>は不適切です。

あちこちのサイトで同じパスワードを設定しておいて，それをメモしてパソコンに貼っておいたら，そのメモを見られただけですぐに被害にあいそうです。だから，<C>の選択は最悪です。

ヒカリちゃんは，どうすればよかったの？

しずかちゃんが教えてくれた方法は，まず，自分には覚えやすくて他人には見破られないパスワードを考えることと，そのときに何かヒントになる文章をもとにすることです。そのヒントを書いたメモを秘密の場所に隠しておけば，かなり完璧ですね。

パスワードを設定する場合のポイントは・・・

1	パスワードは，他人には見破られにくく，自分にとっては覚えやすいものを設定すべし。
2	同じパスワードを設定せずに，サービスごとに違うパスワードを設定すべし。

といったところです。

パスワードの決めかた，覚えかた

他人には見破られにくくて，自分にとっては覚えやすいパスワードを設定するときに，パスワードを覚えられなくても，それを思い出すためのヒントがあればよいのです。

しずかちゃんが教えてくれたような方法で，“私は豆腐がずっと好きです！”というヒントを書いたメモを隠しておいて，もしそれを誰かに見られたとしても，パスワードが“WTsia102G@skDS”だなんてことはわからないでしょう。でも，しずかちゃん本人ならば，“豆腐→102”と“ずっと→@”で置き換えをして，ローマ字で“WATASHIWA102GA@SUKIDESU!”にして，次に数字以外を一つ飛ばしにして“WTSIA102G@SKDS”にしたあと，SHIZUKA（しずか）の文字を小文字にすれば，思い出せるのだそうです。なんだかすごいですね。

パスワードのヒントを書いたメモを誰かにみられることも考える

と，ヒントもそのままに書かないで，“私は■■がずっと好きです！”のように部分的に隠しておくのも良さそうです。メモは，他人に見られない場所で厳重に保管しましょう。パスワードそのもののメモは厳禁で，キャッシュカードや学生証などと一緒にしまうとか，パソコンのそばに貼っておくとか，カードに書いておくというのは最悪です。

メール，ネットショッピングや銀行などたくさんのサービスを使っている人は，同じパスワードを設定しておくと覚えるのは楽ですが，どこかでパスワードが漏れたらぜんぶダメになってしまいます。でも，全部で別々に設定しておくと覚えきれないので，ほどほどに，ですね。

用語解説　「パスワード」

本人の確認や利用資格の確認のために，パスワードが使われます。逆に言うと，パスワードを破られると，他人が成りすますことができてしまうので，パスワードは大事です。銀行のカードでは「暗証番号」と言います。本人だというチェックを「認証」と言います。顔認証，指紋や手の静脈，瞳の模様を使ってチェックする生体認証も使われることがあって，これならば忘れる心配はなさそうです。最近では，パスワードの他に SMS や認証アプリを用いた多要素認証が使われるようになってきました。一度かぎりのメッセージを使う多要素認証もあります。多要素認証が利用できる場合は積極的に使いたいものです。

コラム１ -パスワードのリマインダーの使い方-

パスワードを設定するとき，忘れたときにそなえて本人確認をするための「秘密の質問と答え」を設定できる場合があります。たとえば，生まれたところ，ペットの名前，思い出の旅行先，親の旧姓などの「質問」とそれに対する「答え」をあらかじめ設定しておいて，パスワードを忘れたときに[リマインダー]をクリックすると質問が表示されて，答えが合っていればパスワードやヒントが表示されるというものです。

でも，リマインダーにペットの名前を設定しておいて，ブログでペットを自慢して名前を書いていたら，誰でもリマインダーのチェックを通り抜けられて，あなたのパスワードを知ることができるので，パスワードの意味がなくなります。だから，リマインダーの機能があったとしても，慎重に使わなければなりません。あなたは忘れることがなくて，他人は絶対に知ることがない情報を設定しましょう。一つの方法は，ペットの名前＝“舞浜”（最初のデートに行ったところ）とか，親の旧姓＝“2009.3.5”（自分には忘れられない秘密の記念日）とかを登録して，そのヒントを書き留めておくことです。

コラム2-パスワードは何文字必要？-

パスワードとして意味のある文字の長さは，悪さをしようとする人が想像して試したり総当たりしたりする繰り返しをできる上限回数で決まります。

銀行などは，間違ったパスワードを何度か試すと使えなくしてくれるので，６文字程度でも破られることはなさそうです。一方，ファイルの暗号化に使うパスワードは，手元のパソコンで何万回でもそれ以上でも試し続けられますので，短いと当てられてしまいます。８文字以上で文字や数字などを混在させましょう。

パスワードの文字数と強さの関係

パスワードが数字 1 文字だったら，10 回試せば当てられてしまいます。6～8 文字くらいでかなり安心です。ただし，英単語や人名などは，文字数が多くても辞書を総当たりで試せば破られるので，そのままでパスワードに使ってはいけません。せめて，“MoshiMoshi+KameYo!”くらいの工夫をしましょう。

パスワードに数字とアルファベットや記号などを混ぜると強力になります。パスワードを1文字増やすときに，数字だけのものなら 10 倍当てにくくなるだけですが，数字とアルファベット（大文字小文字），記号を混ぜれば 80 倍くらい当てにくくなります。2 文字増やせば 6 千倍以上です。ファイルの暗号化のように，何度でも試せるパスワードの場合は，コンピュータの性能が日々向上することを考えて，長めで複雑にしておくのがよさそうです。

コラム3-パスワードはときどき変えるの？-

パスワードを半年ごとくらいで変えたほうが良いという説もあります。でも，頻繁に変更すると覚えられないのでメモをすることになり，頻繁に書き換えるメモは管理が悪くなりがちなので，かえって危険性が増すかもしれません。

強固なパスワードを設定しておいて，厳重に管理し，必要になったときにだけ変更するのがお勧めです。

パスワードを変更しなければならないのはどんなとき？

パスワードがあなた個人を確認するためのものならば，絶対に破られないような強力なパスワードを設定しておいて，メモを厳重に保管しておけば，変更する必要はなさそうです。ただし，パスワードを入力した画面を他人に見られたとか，ネットカフェや無線 LAN で無防備のままに入力したあとには，変更しておいたほうが良いでしょう。サービスの利用開始時に“初期パスワード”を変更するのは，不可欠です。

グループでメンバー限定のサーバにアクセスするときに資格確認のために使うパスワードの場合は，メンバー変更があったとか，パスワードが漏れた心配がある時に変更するのは意味があります。ただし，パスワードの通知をほかの人に見られないように注意します。

ネットショップで購入した商品が届かない

第１６話

商品が届かない。どうしたらいい？

ヒカリちゃんは，以前ネットショッピングで偽物のブランドバッグを買ってしまった経験を生かし，今回は慎重にお店を選んでいます。しかし，どうしたことか商品は1週間経っても届きません。メールを調べても注文したあとに何の連絡もありませんでした。ショップの画面で確かめると，未発送の状態です。

このとき，ヒカリちゃんはどのように対応すべきでしょうか。

【問題】　商品が届かない。どうしたらいい？	
A	ショップに問い合わせてみる
B	知り得る窓口に，片っ端から電話をする
C	前に買った偽物のバッグを転売して，穴埋めをする

この場合のヒカリちゃんのとるべき対応は，まずは

A　ショップに問い合わせてみる

ことです。

どうして<A>なのですか？

ネットショッピングとはいえ，ただちに詐欺などのトラブルばかりということはありません。落ち着いて冷静に対応することです。すなわち，まずは商品を購入したネットショップに問い合わせてみることが第一です。販売者に直接連絡がとれないときは，ショッピングサイトの窓口に連絡してみるとよいでしょう。

今回は，販売者に連絡がとれ，数日中には届くとのことでした。販売者はヒカリちゃんにメールで連絡しましたが，ヒカリちゃんがメールアドレスの入力を間違っていたために連絡が届きませんでした。

<B>をやってしまうと？

<B>のようにむやみに騒いでもほとんど解決にいたりません。

<C>をやってしまうと？

<C>のように偽物であることを知りながら本物として販売すると，詐欺罪（刑法 246 条）という犯罪になる可能性がありますので，注意してください。

ポイントは・・・

1	何かトラブルになりそうだったら，まずショップやモールの受付に確認する。
2	ショップで解決できず，悪質だと思われるものに関しては警察や消費生活センターに連絡。
3	もし偽物と知りながら販売してしまうと，犯罪になるので注意が必要。

ネットショッピングの欠点

街の店舗での買い物では，商品を手に取って吟味し，レジでお金を支払いますが，ネットショッピングではこれらの手順をすべて画面上で行うため，さまざまなトラブルの可能性があります。たとえば，送金したのに商品が届かない，商品は届いたが偽物だったり，期待したものと違っていた，注文のときに入力した個人情報が漏えいしてしまったなどのトラブルです。

こうしたトラブルを防ぐため，ネットショッピングを利用する場合は，お店やお店が出店しているショッピングサイトが信用できるかどうか，手数料・送料・消費税の扱い，代金の支払い方法，商品の引き渡し方法，返品の可否などの販売条件について，あらかじめしっかりと確認しておく必要があります。

ネットショッピングのトラブル対策

ネットショッピングを利用するときは，ネットショップのショップ名，住所，電話番号，担当者名，連絡先など（特定商取引法に基づく表記のページ)を控えておきましょう。後日ショッピングサイトが突然消えてしまい，連絡が取れなくなる場合があります。注文

画面や注文確認のメールは，スクリーンショットやプリントアウトするなどして商品が届くまで保管しておきましょう。後で，警察や消費生活センター等に相談するときに役立ちます。

なお，最も単純なトラブル対策としては，名前がよく知られたネットショップを利用するという方法があります。著名なネットショップであれば，そうした販売条件が整備されていること，誇大や不適切な広告表現がないこと，個人情報が適正に管理されていること，トラブルが生じたとき確実に連絡が取れることなどが期待できるからです。また，本や CD など一般に広く出回っている商品の方が無難です。中古品や特定物を購入しようとするときは，特に注意が必要です。

支払いに注意

取引相手が信用できないと思われる場合は，できるだけ料金の先払いは避けるべきです。料金を支払っていなければ，たとえ商品が届かなかった場合でも金銭的被害は生じません。

ネットショッピングで代金を支払う場合は，正規のサイトの支払い画面であることを必ず確認します。また，利用者を偽の画面に誘導してクレジットカード番号等を盗み出すフィッシング詐欺の危険もありますので，代金支払いの場面では注意が必要です。

入力情報は間違えないように！

どうしてヒカリちゃんには連絡が届いていないのでしょう。ネットショッピングでは，注文の際，電子メールアドレスなどの個人情報を入力しますが，それが間違っていたのかもしれません。ちなみに，注文個数の入力ミスや予約の日付入力ミスなども考えられ

ますから，入力に間違いがないか，慎重に確認する癖をつけておきましょう。

連絡がとれないような悪質な場合は？

ネットショップに何度問い合わせても連絡がとれないような悪質な場合は，注文画面をプリントアウトしたものなどを用意した上で，警察や消費生活センター等の公的な相談窓口に問い合わせみてください。以下に，参考となるリンクを挙げておきます。

- 都道府県警察本部のサイバー犯罪相談窓口等一覧（警察庁）
  http://www.npa.go.jp/cyber/soudan.htm
- 全国の消費生活センター等（国民生活センター）
  http://www.kokusen.go.jp/map/index.html

コラム-注文は取り消せますか？-

訪問販売にはクーリング・オフ制度があります。クーリング・オフとは，一定の期間内であれば書面によって申込みの撤回や契約の解除ができる制度です。通信販売にはこのクーリング・オフがありません。ネットショッピングも通信販売と同様の取引形態と考えられますので，クーリング・オフはできません。

ただし，ネットショップによっては返品が可能な場合がありますので，注文する前に返品の可否と返品可能な場合の条件と返品可能期限をよく確認しましょう。

操作ミスの場合は契約を無効にすることができる

インターネットショッピングで，「買う商品を間違えた」「数量を間違えた」「購入画面が不明瞭で何度も購入ボタンを押してしまった」などの場合は，法律上の「錯誤」にあたり，契約を無効とすることができます（民法 95 条）。ただし，消費者側に著しい不注意（重過失）があったときは，契約の無効は主張できないとされています。

しかし，ネットショッピングの場合は，電子消費者契約法（電子消費者契約及び電子承諾通知に関する民法の特例に関する法律）によって，ショップ側が確認画面を表示して消費者の意思を確認したような場合を除いて，重過失で操作ミスや入力ミスをしてしまったときでも，無効を主張できるようになりました。

ネットオークションやフリーマーケットの落とし穴

ネットオークションやフリーマーケットでは，取引相手は個人ですから，信用できる相手かどうかを判断するのは困難です。出品者の評価や過去の出品リスト，連絡先などをよく確認するようにしてください。また，オークションでは決まった値段がないので，繰り返し入札しているうちに思わぬ高値で落札してしまうこともあり，注意が必要です。ネットショッピングに比べて，詐欺などのトラブルも多いようです。そのほか，海賊版販売，偽ブランド品や盗品，違法物品の取引に利用されるケースもありますので，十分に注意してください。

パソコンの正しい捨て方

第１７話

捨てるときにも作法がある

つばさくん，使っていたパソコンが壊れたのをきっかけに捨てることにしたようです。ただし，テレビのニュースなどでときどき話題になる「情報漏洩」が，パソコンを捨てることによって起こることも知っているようで，ちょっと不安そうですね。きれいさっぱり捨てたいときには，どうするのがよいのでしょうか。

さて，ここでいつもの３択問題です。

【問題】　パソコンを捨てるつばさ君は，本当はどうすればよかったのでしょう？	
A	粗大ゴミか，資源ゴミの日に出すなど，各自治体の定めに従う
B	パソコンは，捨てる前に，綺麗に掃除する
C	専用ソフトを使いパソコンのデータを消去してリサイクルに出す

この場合のつばさ君の選ぶべき答えは

C	専用ソフトを使いパソコンのデータを消去してリサイクルに出す

です。

どうして<C>なのですか？

パソコンの中に入っているハードディスクや SSD には，パソコンを使っていたときに記録されていたデータが残っています。これをそのまま捨てると，後から拾った人が中身を見ることができてしまいます。ファイルの削除やフォーマットをしても，完全には消えないのです。なので，専用ソフトで完全にデータを消してからリサイクルに出すことが必要です。

どうして<A>と<B>は間違いなのですか？

まず，パソコンは「資源の有効な利用の促進に関する法律」（資源有効利用促進法）でメーカーによる回収・リサイクルが義務づけられていますので，自治体の回収に出すことはできません。さらに，ゴミとして出しただけでは，つばさくんの心配しているデータの消去はできません。こうした理由で<A>は不適切です。

一方，<B>についてはパソコンを外から掃除するだけですので，もちろん意味がありません。箱の中を開けてほこりを掃除しても同じです。だから，<B>を選択することももちろん不適切です。

つばさ君は，どうすればよかったの？

「データの完全削除」ができるソフトウェアが販売されています

（無料のものもあります）ので，これを使用します。操作は難しくありません。もっとも，ハードディスクの故障が原因でパソコンが壊れている場合はこうしたソフトは使えませんので，ハードディスクを物理的に壊すしかありません。

パソコンを捨てる場合のポイントは・・・

1	パソコンを捨てる際のデータ消去は，専用ソフトを使用して実施すべし。

といったところです。

消えていないファイルの怖さ

ハードディスクやUSBメモリなどに入れたファイルは消去すると「ごみ箱」に入れられ，「ごみ箱を消去」すると完全に消えたように見えます。しかしこの場合ですら，ファイル復活ソフトウェアを利用すると，高い確率でファイルを元に戻すことができます。

さらに困ったことに，中古のパソコンや捨てられたパソコンのハードディスクから，この種のソフトウェアを使ってファイルを復活させ，プライベートな写真などを収集する悪趣味な行為が一部で行われています。これを防ぐために，パソコンを手放したり捨てたりする前には，ハードディスク等を確実に消去することが必要なのです。

コラム１-データ完全削除ソフト-

パソコンを廃棄する時に使用するデータ完全削除ソフトは，2000 円から 1 万円を超えるものまで色々あります。ただ，そんなに頻繁に使うものではないので，市販のものはど～もという人は，フリーソフトもありますので，それを使うといいでしょう。市販ソフトの中には大事なデータを誤って削除した時のデータ復元ソフトとペアになったものもありますので，一つ持っていると便利です。

データの削除にいくつも方式があるのはなぜ？

データ完全削除ソフトでは，「どのレベルで消すか」を選べるものが多いようです。これは，ハードディスクに何度も書き込むほど，データを復活させにくくなる代わりに，長い時間がかかるため，データの重要度に応じて選べるようになっているのです。なぜ何度も書き込むかというと，ハードディスクは磁力を応用してデータを記録しているので，新しいデータを書き込んでも，前のデータの特徴が微弱な磁力（これを残留磁気といいます）として残ってしまうためです。アメリカの国家安全保障局（NSA）が定めている方式では，でたらめなデータを2回書き込んだ上で，さらにもう1回ゼロを書き込むことになっています。こうすると，元のデータを読むには4回前の磁力を探ることになるため，高度な技術をもったスパイ組織でも復活させることはできないというわけです。逆に，スパイに狙われるようなデータでなければ，もっと低いレベルでも実用上は問題ありません。

一方，専用ソフトの中には，データをゴミ箱から削除するタイミングで自動的に上書きしてくれる機能を持ったものがあります。こ

のような機能を使用しておくとパソコンを廃棄する時も安心です。

暗号鍵を破壊することで一瞬で読めなくするハードディスク

最近，暗号化チップ付のハードディスクが登場しています。これはハードディスクにデータを書き込むときに，つねに暗号化チップを使って暗号化しているので，暗号化チップに格納されている鍵が無いと中身を読むことができません。こうしておくと，ハードディスクを廃棄する時，暗号鍵を破壊することで，一瞬にしてデータを読めなくすることができます。

コラム２
-ハードディスクを物理的に破壊するには-

ハードディスクはデータを保護するため，多くの部分が金属でできていて物理的に破壊するのは大変です。

ドリルやハンマーで壊す人もいますが，簡単には壊れませんし，ドリルの刃が折れたりするので危険です。

どうしても破壊したいという人は事故のないように気を付けてください。

ハードディスクの破壊は注意して

最近は多くのハードディスクを完全に消去するには，個人の場合，一番手軽な方法は専用のソフトウェアを使う方法です。しかし故障してしまったパソコンを廃棄する場合はそうはいきません。ハンマーやドリルで破壊するのも器具に不慣れな人には危険です。

データを完全に消すには

困ったときはパソコンのリサイクルを専門に扱う業者に相談しましょう。業者側で物理的に破壊する機械を使ってくれる場合があります。どうしても自分で行う場合は，コラムにあるような方法で壊すことになります。

コラム３-パソコンの廃棄とリサイクル-

消去したハードディスクや，物理的に使えなくしたハードディスクは，リサイクルしても大丈夫です。

実はハードディスクなどの電子部品には，世界的に埋蔵量の限られた金属（レアメタル）が使われているので，不燃ゴミとするのは非常にもったいないことなのです。

パソコンメーカーの行っている回収に出すと，こうした資源を再利用することができますので，不燃ゴミなどに出さず積極的にリサイクルしてください。

セキュリティ演習の課題を試したい

第１８話

セキュリティ演習の課題を家で試していいの？

ヒカリちゃんとしずかちゃんは，ネットワークセキュリティ演習の授業をうけていて，今日は演習専用のウェブサーバに特殊な入力を送って誤動作する様子を観察する課題でした。ヒカリちゃんは授業時間内にうまくできなかったので，うちに帰ってからやってみようと考えています。でも，しずかちゃんは，家からやっても良いのか，心配しているようです。

さて，ここで３択問題です。考えてみてください。

【問題】　ヒカリちゃんは，ウェブサーバを誤動作させる演習と同じことを，家からインターネット上のウェブサイトに試してもよいのでしょうか？	
A	自分が契約しているウェブサイトで試せば，問題ない。
B	実際のウェブサイトで試すのは，ぜったいにダメ。
C	課題を実践して体験するのが大事なので，やるべき。

この場合のヒカリちゃんの選ぶべき答えは

B 実際にウェブサイトで試すのは，ぜったいにダメ。

です。

どうして<B>なのですか？

ネットワークセキュリティ演習の授業は，特殊な入力を送って誤動作させるための演習専用ウェブサーバを先生が用意して，誤動作する様子を観察する課題でした。管理者からの許可をあらかじめ得ずに，ウェブサーバなどの情報システムを誤動作させたりデータにアクセスしたりすることは攻撃に相当する行為です。

演習で取り上げるような攻撃手法はすでによく知られたもので，インターネット上のウェブサーバでは攻撃が成功しないような対策が済んでいるはずです。しかし，もし対策ができていなければ攻撃してしまったことになりますし，対策がちゃんとできていて攻撃が失敗したとしても攻撃を試みたとみなされるかもしれません。攻撃することやその試みをすることは，ほとんどの場合は犯罪になってしまうので，絶対に試してはいけません。

どうして<A>は間違いなのですか？

自分が契約しているウェブサービスでも，そのウェブサーバに攻撃を仕掛けたら，犯罪とされる可能性があります。自分が賃貸契約している部屋であれば何をしてもよいわけではないことと同じです。自分が契約しているウェブサイトだとしても，攻撃が許されるとは考えられませんから，<A>は間違いです。

なお，当然ですが，契約していないウェブサービスに対しても同

様です。たとえば，ウェブ検索サイトの検索語の入力欄に，演習で用いた特殊な文字列をそのまま試しに入力したりしてはいけません。

どうして<C>じゃだめなのですか？

大学の授業で習ったことを，帰ってから反復学習することは良い心がけです。ただし，ネットワークセキュリティ演習では学生の安全や大学内外への影響を考慮して実践体験する内容を決め，学生の操作が攻撃や犯罪にならないように配慮して計画し，そのために用意した環境の中で実施します。教室外や演習時間外に試すことは攻撃とみなされるおそれがあるので，<C>は不適切です。

コラム１-不正アクセスとサービス妨害-

あらかじめ許可を与えられた利用者ではないのに情報システムやデータにネットワークからアクセスすると，不正アクセスとして犯罪とされます。

また，サーバを攻撃して誤動作させ，あるいは性能低下や停止させることをサービス妨害といい，犯罪とされます。たとえ，金銭的あるいは政治的などの目的がなくて興味本位だったとしても，許されません。

ヒカリちゃんは，どうすればよかったの？

ネットワークセキュリティ演習の先生は，課題で示した特殊な入力を送れば誤動作して，その様子を観察できるようなウェブサーバを用意していたはずです。そのサーバ以外で，演習と同様のことをしてはいけません。ヒカリちゃんは，演習の時間内に演習専用のウェブサーバでやっておくべきでした。

攻撃手法をネットで試すのもだめ

ヒカリちゃんたちの授業では，今回の演習のほかにも，不正アクセスの原因になるぜい弱性や，コンピュータウイルスの動作原理についての講義があるかもしれません。それは，情報セキュリティ問題を理解して対策を考えるために必要な知識であって，それを使ってインターネットで試したり，あるいは悪用して犯罪に走ってはいけません。

また，インターネットで検索し入手できる情報には有益なものが多くありますが，なかには様々な法律に違反するもの，国によって違法とされる有害な情報もあります。とくに，情報セキュリティに関係する情報を検索して調べていると，リスクの説明や対策方法などの注意喚起情報のほかに，具体的な攻撃手法を手に入れられるウェブサイトをみつけてしまうこともありえます。

攻撃手法の情報を見てしまうと試してみたくなる興味がわくかもしれませんが，インターネットでどこかのウェブサーバなどに対してそれを試してしまうと，攻撃を試みたことになり，犯罪とされる可能性もあります。情報検索するときには自制心をもちましょう。

また，違法な情報などを集めて掲載するウェブサイトでは，ウェ

ブページや広告に擬装してコンピュータウイルスなど有害なプログラムを送り込んでくるようなところもあり，表示するだけでも危険性があるので，アクセスしないように警戒するべきです。

コラム２-ウェブサイトの弱点を見つけたら-

インターネットを使っていて，攻撃への対策が不十分なウェブサイトに気づくことがあるかもしれません。（くどいですが，試して探してはいけません。）そのようなときは，誤動作を確かめたり，そのことを SNS に書いたりするのは，絶対にいけません。サーバに対策をしていないのが悪いのだから，そのことを言い広めたり攻撃したりしてよいということにはなりません。

インターネット社会の一員としては，セキュリティの向上に貢献できるよう，経済産業省の告示に基づく届出窓口に報告しましょう。

情報処理推進機構（IPA）の届出・相談・情報提供窓口：
https://www.ipa.go.jp/security/outline/todoke-top-j.html

2018 年版のあとがき

「ひかり＆つばさの情報セキュリティ 3 択教室」が世に出てから９年が過ぎました。この間，サイバーセキュリティ基本法の成立，個人情報保護法や著作権法の改正，「政府機関の情報セキュリティ対策のための統一基準」といった情報セキュリティをめぐる環境の激しい変化があり，情報セキュリティやサイバーセキュリティという言葉が新聞等で日常語として扱われるようになっています。

時代の変化に合わせて学生向けの情報セキュリティ教材「ひかり＆つばさの情報セキュリティ３択教室」の改訂を検討していましたが，２０１７年度に旧版に大幅に加筆・修正をして２０１７年末に編集委員会をもち２０１８年版を完成しました。

読んでみた感想，要望等をいただければ幸いです。

２０１８年版編集代表
中京大学　長谷川　明生

編集作業委員会（2017 年 12 月）
とりまとめ：長谷川明生（中京大学）
委員：須川賢洋（新潟大学）
　　中西通雄（大阪工業大学）
協力：曽根秀昭（東北大学）
　　冨田高樹（みずほ情報総研）

執筆いただいた方々（旧版および 2018 年度版）50 音順
上田浩（京都大学）
上原哲太郎（立命館大学）
岡田仁志（国立情報学研究所）
岡部寿男（京都大学）
小川賢（神戸学院大学）
金谷吉成（東北大学）
木下宏揚（神奈川大学）
佐藤慶浩（オフィス四々十六）
須川賢洋（新潟大学）
曽根秀昭（東北大学）
冨田高樹（みずほ情報総研）
長谷川明生（中京大学）
冨士原裕文（富士通株式会社，執筆時）
丸橋透（富士通フロンテック）

この教材の利用ルールについて

■ 本書は、原則として著作権法 35 条に定める範囲に沿って使ってもらうこと想定しています。その上で、本書を大学（短期大学、高等専門学校等の高等教育機関を含む）の教員が大学の講義で使用することは差し支えありません。

■ 学内の教職員、学生に対して複製して配布しても構いません。

■ また、本書の内容を大学内からのアクセスに限定されたサーバー、あるいは学内の教職員、学生にアクセスが制限されたサーバーから複製することは差し支えありません。

■ 大学の講義のほか、FD・SD や学生向け講習会等で本書を使用・複製することは差し支えありません。

■ 本書の内容を，営利目的で使用することはできません。

■ 本書を，以下の条件のもとで学内向けに改変・追記して使用することを認めます。
① 原作者のクレジット（氏名，署名等）の表示部分は改変せず残す。
② 読者が改変・追記した版を原版と誤解することのないように，改変・追記したものである旨を明示する。
③ 改変・追記したものを学外に公表しない。

■ 本書の一部を学内向けの教材等に使用する場合は，当該教材内で本書を使用した旨を明示してください。本書の一部を使用した教材等を学外等で使用したい場合はご相談ください。

■ 地域連携・高大連携などを目的とした使用につきましては、本書の内容が主として大学の学生・教職員を対象としておりますことから、大学以外の方に向けた教材としては作成されていません。ただし、ご了承のうえ使用していただくことは差支えありません。

■ なお、大学外での使用につきましては、原則としてご遠慮いただいておりますが、個別の事案によってはご相談のうえ利用いただける場合もございますので、ご希望がありましたらご相談ください。

■ お問い合せ先
国立情報学研究所 高等教育機関における情報セキュリティポリシー推進部会：
sp-comment@nii.ac.jp

ヒカリ＆つばさの情報セキュリティ3択教室 ＜2018 年版＞

2009 年 3 月 31 日　初版（CD・書籍版）発行
2018 年 3 月 1 日　2018 年版（PDF 版）発行
2018 年 12 月 1 日　2018 年版（第 18 話追加 PDF 版）発行

編著　岡田 仁志
発行　国立情報学研究所
〒101-8430 東京都千代田区一ツ橋 2-1-2
学術総合センタービル
03-4212-2000 （代表）
https://www.nii.ac.jp