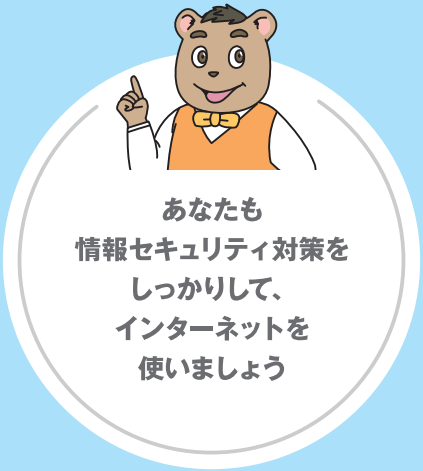


あなたも
情報セキュリティ対策を
しっかりして、
インターネットを
使いましょう

知る 守る 続ける

NISC 内閣官房情報セキュリティセンター
National InFormation Security Center

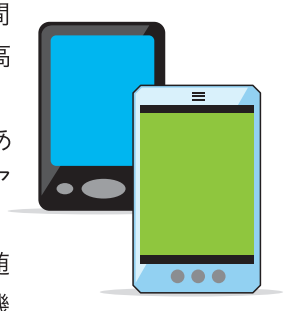
国民を守る情報セキュリティサイト
http://www.nisc.go.jp/security-site/

ASEAN・JAPAN
Information Security Awareness

知る 守る 続ける 情報セキュリティ

安心してインターネットを使うために

スマートフォンについて



世界規模で、**スマートフォン**の普及が進んでおり、年間の携帯電話販売台数に占める**スマートフォン**の割合も高まってきています。

スマートフォンは、従来の携帯電話に比べて高機能であり、パソコンと同じウェブサイトを閲覧できるほか、様々なアプリケーション※1をダウンロードして、自由に利用できます。

また、**スマートフォン**のOS※2やアプリケーションは、随時アップデート※3版が提供され、これにより、更なる高機能化やセキュリティ対策も可能です。

※1 文書の作成や数値計算など、ある特定の目的のために設計されたソフトウェアです。
どのソフトウェアにも共通する基本的な機能をまとめたOSに、ユーザーが必要とするものを組みこんで利用します。

※2 オペレーティングシステムの略称で、パソコンやスマートフォン全体を管理するためのソフトウェアです。たとえば、パソコンでは、キーボードの入力やディスプレイ、プリンタへの出力といった入出力機能などの管理を行っています。

※3 アップデートとは、ソフトウェアの小さな更新のことをいい、不具合の修正や、機能向上などの提供のため行われ、これによりソフトウェアを最新の状態に保つことができます。セキュリティソフトについても、アップデートが大切です。

危険ポイント

1 **スマートフォン**を対象としたウイルスが増加しています。ウイルスに感染すると、電話帳の中身などの外部送信や不正課金などの被害が起こるおそれがあります。

2 ウイルスの感染以外に、アプリケーションをダウンロードする際に、端末情報や電話帳の中身など、本来必要のない情報の利用許諾を求め、外部のサーバに送信しようとする場合があります。例えば、電池を長持ちさせるためのアプリケーションと称して、本来必要のない電話帳情報を外部に送信しようとするものも存在します。

注意点と対策

- **スマートフォン**のOSやアプリケーション、ウイルス対策ソフトは常に最新のものにするよう心がけましょう。**スマートフォン**は、電話帳情報など多くの個人情報が記録されていることが多いため、パソコンに比べても、更に注意が必要です。
- アプリケーションのダウンロードの際には、信頼できるサイトかどうか、アプリケーションの提供元はどこかなどを確認するようにしましょう。また、ダウンロード時には、利用許諾画面や利用規約などで、収集される情報の範囲や利用目的などをよく確認した上で、同意・利用するよう努めましょう。

無線LANのセキュリティについて

近年、パソコンの軽量化やスマートフォンの普及が進み、家やオフィス、又はその外でも、無線通信を利用してインターネット接続を行う「**無線LAN**」の利用が増えてきました。

プロバイダによる有料サービスに加えて、空港、駅、商業施設などでの無料の公衆**無線LAN**サービスも増えています。

危険ポイント

1 家やオフィスの**無線LAN**は、電波の届く範囲で自由に接続が可能なため、適切なセキュリティ対策を行わないと、通信内容が第三者に盗み見られるおそれがあります。また、**無線LAN**ネットワークに不正に侵入され、個人情報や企業秘密が漏えいしたり、サイバー攻撃の踏み台にされたりするおそれがあります。

2 公衆**無線LAN**サービスでは、パソコンやスマートフォンが偽のアクセスポイント（親機）に接続してしまうおそれがあります。その場合、**無線LAN**が暗号化されていても、通信内容が盗み見られたりするおそれがあります。

注意点と対策

- 家やオフィスの**無線LAN**は、通信内容を盗み見られたり、第三者に接続されないよう、データの暗号化設定（WPA2：Wi-Fi Protected Access 2など）を確実に行いましょう。暗号化の設定を手動で行うときは、十分に長いランダムな文字列を暗号鍵に設定しましょう。
- 公衆**無線LAN**サービスを利用する場合は、SSL※4で暗号化されたウェブサイト（URLがhttps://で始まるサイト）しか使わないようにしましょう。また、接続するパソコンのファイルの共有の設定がオフに設定されているか、確認してから利用するようにしましょう。

※4 Secure Socket Layerの略で、インターネット上でやり取りするデータを暗号化するための仕組みのことです。

ワンクリック詐欺について

ワンクリック詐欺とは、ウェブサイト上の画像や動画などをクリックするだけで、料金請求画面が突然表示するなどして、入会料やサービス使用料などの名目で支払いを要求し、金銭を騙し取る詐欺のことをいいます。

最近では、スマートフォンのアプリケーションや、ブログ※5・SNS※6などのソーシャルメディアを悪用した**ワンクリック詐欺**も現れています。

「ワンクリック」のケースだけでなく、年齢確認など複数回のクリックの後に請求画面を表示するケースや、電源をシャットダウンしても請求画面が消えないケースなど、手法が悪質化・巧妙化してきています。

※5 ウェブログ（Weblog）の略で、自分の意見や感想を日記風に記して、それに対する感想などを閲覧者が自由にコメントできる形式のウェブサイトです。

※6 SNSとはソーシャル・ネットワーキング・サービスのアルファベットの頭文字をとったもので、個人の日記やフォトアルバムを特定の人に公開できたり、利用者同士が気軽に意見交換できるコミュニティを開設できたりなど、様々な機能を持ったウェブサイトを提供するサービスです。

危険ポイント

1 ユーザーの関心を惹く無料の画像や動画などをダウンロードしようと、安易にクリックすると、不正な請求を受けたり、詐欺サイトに誘導されたりするおそれがあります。

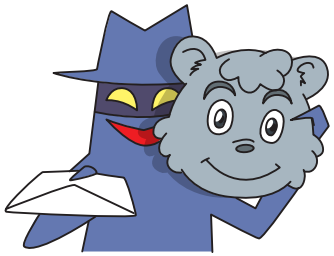
2 請求画面に端末のIPアドレス※7や利用プロバイダを表示し、あたかも個人が特定されているかのように錯覚させて、不安を煽るケースもあります。

※7 インターネットに接続するコンピュータや機器に、通信の接続時、自動的に割り振られる識別番号のことです。

注意点と対策

- フィルタリングソフトや、最新のセキュリティソフトを活用し、不正なウェブサイトへの誘導をブロックするようにしましょう。また、スマートフォンのアプリケーションは、信頼できるサイトからダウンロードするようにしましょう。
- パソコンでは、クリックしただけでは、個人が特定されることはないので、不安になって料金の支払いに応じることのないよう、注意しましょう。なお、スマートフォンでは、アプリケーションによっては、自らの連絡先や電話帳など端末に記録された情報が流出するおそれがありますので、注意しましょう。
- 連絡を取ってしまったり、不正な請求が続いたりする場合や、裁判所からの通知などがあった場合には、関係機関（行政相談や弁護士の無料相談など）に相談しましょう。

標的型メール攻撃について



標的型メール攻撃とは、知人などを装って偽のメールを送り、その添付ファイルなどでウイルスを感染させるものです。

標的とした特定の企業や個人ユーザーに向けて、関係者や別の社員などを装ってウイルスメールを送信する攻撃が典型例です。

最近も**標的型メール攻撃**によって、個人のパスワードなどが詐取されたり、ウイルス感染したりするなどの被害が報告されています。

危険ポイント

1 最近では、送られてきたメールを信用させるため、実在する部署や社員の名前などを記載したり、仲間内でしか知らない内容でメールを作成したりするなど、手口が巧妙化、高度化してきており、攻撃の成功率を高めています。

2 ウイルスが添付されている場合は、添付ファイルを開くだけで、自動的に外部コンピュータに接続してしまい、知らないうちにコンピュータ内部の情報が抜き取られて外部に勝手に送信されてしまいます。

注意点と対策

- 心当たりのないメールの添付ファイルやURLは開かないようにしましょう。
- もし、不審なメールを開いてしまったら、落ち着いて、電源は切らず、コンピュータに接続されているネットワーク用ケーブルを抜いた後に、身近にいるシステム管理者などに相談・連絡しましょう。
- ウイルス対策ソフトを導入し、常に更新しましょう。
- OSだけでなく、アプリケーションの更新もこまめに行いましょう。

DDoS攻撃について

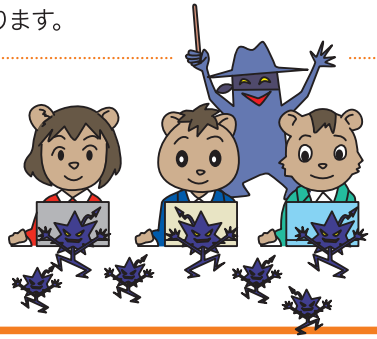
DDoS[※8]攻撃とは、複数のネットワークに分散する大量のコンピュータが、ウイルス感染などにより、一斉に特定のサーバへパケットを送出させることで、通信路をあふれさせて機能を停止させる攻撃です。

※8 Distributed Denial of Serviceの略

危険ポイント

1 攻撃者は、攻撃対象とは無関係な多数のコンピュータに侵入して攻撃実行用のプログラムをこっそりしかけるため、一般ユーザーは気づかないうちに他人のパソコンを攻撃してしまうことになります。

2 感染したコンピュータは、**DDoS攻撃**以外にも、ウイルス感染活動や迷惑メール送信、ウェブサイトの改ざんなど多岐にわたって利用され、他のサイバー攻撃の手助けとなってしまいます。



注意点と対策

- パソコンやスマートフォンなどネットワークに接続する機器のOSは常にアップデートして最新の状態にしましょう。
- ウイルス対策ソフトを導入し、常に最新の状態にしましょう。
- OSだけでなく、アプリケーションの更新も行いましょう。

インターネット利用のマナーについて

SNS（ソーシャル・ネットワーキング・サービス）の利用拡大に伴い、いままで想定されなかったネット上のトラブルが発生しています。

個人によるネットへの書込みによって、本人が特定され中傷を受けたり、企業が謝罪を行う事態に発展したりするなどの事案も起こっています。

危険ポイント

1 SNSなどでの何気ないネットへの書込みによって、自分の個人情報が外部に流出したり、他人の名誉棄損、プライバシー侵害をひき起こしたりするおそれがあります。

2 いたずらや軽い気持ちによるネットへの書込みであっても、場合によっては損害賠償を請求されたり、法律による処分を受けたり、逮捕される可能性もあります。

注意点と対策

- SNSやブログ、ミニブログなどを含め、インターネット上でむやみに個人情報を公開しないように気をつけましょう。これらに掲載した写真などから位置情報まで判明する場合があり、注意が必要です。
- また、インターネット上でも、他人の尊厳やプライバシーに配慮し、内容をきちんと確認してから情報発信を行うようにしましょう。

ID・パスワードの適切な設定・管理について

電子メールや、ネットショッピング、ネットバンキングなど、インターネット上のサービスを安全に利用するために、様々な認証方式が用いられていますが、最も一般的なものとして、**ID・パスワード**があります。

近年、**ID・パスワード**などのユーザーアカウント情報の窃取を目的としたサイバー攻撃が増加しています。

危険ポイント

1 安易な**パスワード**（誕生日４ケタの設定、「9999」など）を用いたり、ずさんな管理（付箋に**パスワード**を記載してパソコンに張り付けるなど）をしていると、悪意のある第三者に不正アクセスされて利用者本人になりすまされ、個人情報漏えいや金銭盗難などの被害に遭うおそれがあります。

2 複数のサイトで、同一の**ID・パスワード**を使い回していると、１つのサービスで漏えいした**ID・パスワード**により、他のサイトで不正アクセスの被害に遭うなど損害が大きくなる可能性があります。

注意点と対策

- **パスワード**は、推測されにくい、数字・文字・記号を全て含む8文字以上のできるだけ長くてランダムな文字列を設定し、定期的に変更しましょう。
- **パスワード**を他人に知らせたり、複数のウェブサイトで同一の**パスワード**を用いることは避けましょう。自分が利用しているサイトから「**パスワード**が流出した」との通知があった場合は、そのサイトの**パスワード**を変更するだけでなく、同一の**パスワード**を設定している他のサイトの**パスワード**も直ちに変更しましょう。
- インターネットカフェなどの不特定多数の人間が利用するコンピュータで、個人情報や機密情報を入力することは避けましょう。

迷惑メールについて 1

電子メールは、相手の所在の有無や、相手との距離の大小を気にせず、受発信が可能な、利便性の高いコミュニケーション手段である一方、受信者にとって不要なメールが大量に送受信される場合もあります。

迷惑メールが大量に送信されることにより、プロバイダの設備に過度の負担がかかり、他のメールの送受信に遅延が生じるなどの問題も起こっています。

危険ポイント

1 コンピュータでランダムに大量のアドレスを作成し、無作為にメールを送信している場合があるため、短い文字数のアドレスや、一般的な名前をそのまま使用したアドレスは、**迷惑メール**の配信対象となる可能性が高くなります。

2 架空の無料サービスへの登録や、虚偽の配信停止手続きなどにより、有効なアドレスを収集し、**迷惑メール**送信に用いている場合もあります。

注意点と対策

- メールアドレスは、文字数が長く、英数字をランダムに混ぜるなど、推測されにくいものにするようにしましょう。
- インターネットのサイトに、自分のメールアドレスをむやみに入力したり、公開したりすることは避けましょう。
- 信頼性が確認できないサイトなどを用いなければならない場合には、メインのプロバイダのアドレスの利用を避け、フリーメールアドレスを利用するなど、メールアドレスを使い分けることも有効です。

迷惑メールについて 2

迷惑メールは、受信者を不愉快にさせたり、業務の妨げになったりするだけでなく、金銭を騙し取るために不正なウェブサイトに誘導するもの、**迷惑メール**フィルターを通過するものなど、悪質・巧妙なものが増えています。

迷惑メールをきっかけに、スマートフォンがウイルスに感染し、外部から遠隔操作され、知らない間に**迷惑メール**の大量送信を行ってしまうケースも出ています。

危険ポイント

1 **迷惑メール**本文中のリンクにアクセスすると、不正なウェブサイトに誘導されたり、ウイルス感染のきっかけとなる可能性があります。

2 スマートフォンの普及が進むにつれ、パソコンと同様のメールを受信することができるスマートフォンでも、**迷惑メール**の被害に遭うリスクが増えています。

注意点と対策

- 受信拒否機能やなりすまし拒否機能などのプロバイダの**迷惑メール**対策サービス、フィルタリングソフトなどを活用し、**迷惑メール**をできるだけブロックしましょう。
- **迷惑メール**を受信した場合には、開封せずに削除しましょう。また、不審なメールに添付されているファイルや、リンクにアクセスすることはやめましょう。プロバイダや公的機関に、**迷惑メール**を申告（転送）することも有効です。
- スマートフォンでも、パソコンと同様の**迷惑メール**対策を行いましょう。

自分で守ろう スマホやパソコン

スマートフォン、パソコンは便利な反面、
コンピュータウイルス感染等の危険もいっぱい。
パソコンやスマートフォンを安全に、
安心して使えるようにするため、
情報セキュリティ対策3か条を守りましょう。

情報セキュリティ対策3か条

個人情報等の重要な情報の扱いは慎重に

パソコン等は常に最新のセキュリティ状態に

不審なサイトやメールにアクセスしない

情報セキュリティ対策は、たとえるなら、自動車に乗るときにはシートベルトを締めるのと同じで、パソコンやスマートフォンを使うときに忘れてはならないものなのです。