



# ケーブルインターネット

by ChunChunNet

## のセキュリティ

最近よく、「セキュリティ」という言葉を耳にするようになりました。私たちは、普段生活の中で何の抵抗なく使用していますが、その言葉の意味はご存知でしょうか？辞書で引いてみると、「安全」、「安心」、「油断」、「確実」、「保護」、「防衛」などといった語句がありました。

インターネットの世界でみると、「インターネットセキュリティ」といった言葉になります。この言葉の意味を先ほど辞書の語句の中から選べと言われたら、「防衛」という語句が一番ふさわしいのではと思います。おそらく多くの方は、「安心」「安全」だろうと、想像されたと思いますが、これから述べる事でその意味を理解して頂けると幸いです。

### はじめに

インターネットを利用するという事は、世界中の情報が自宅に居ながら収集でき大変便利ではありますが、その反面、「**不特定多数の人から接続できる**」という環境でもあるという事を認識しておきましょう。その不特定多数の人は、「**一人の人間**」であり、そのすべての人が善人だといいいのですが、「**大部分が見えない世界**」になっている事を十分に認識した上で利用しないと、後で大変な事になりかねません。インターネットの世界においては、「**規則や秩序が十分に整っていない環境**だ」という事を利用する側も十分に理解しておきましょう。

又、インターネットを利用する中で、「必ず自己責任をお願いします。」と決まりごとのような文句がよく見受けられます。それらを意味するものは、「**自分の身は自分で守る**」という事がインターネットの世界では当たり前とされるケースが多いからです。そうした文面を見たときには、「何も保障されていない」という事をよく認知しておく事が大切です。

では、一言に「守れ、守れ」といわれて、一体何からはじめて、何をしたらいいのか？多くの方はそう感じられるかもしれません。「何から」守る？と考えると少し分かりやすいかもしれませんが、その「何から」には「危険」があたります。その「危険」には、どういったものが考えられるのか？ブロードバンド(広帯域、大容量、常時接続といった意味)接続環境下での危険性とその対策について、簡単ではありますがご説明いたします。

注)これらは、ほんの一部に過ぎない事であり、今後、ご利用していく環境の変化などで十分でない事を前提とします。

そうした環境の変化の中でも、自己防衛対策の足がかりになれば幸いです。



# ケーブルインターネット

by ChunChunNet

## のセキュリティ

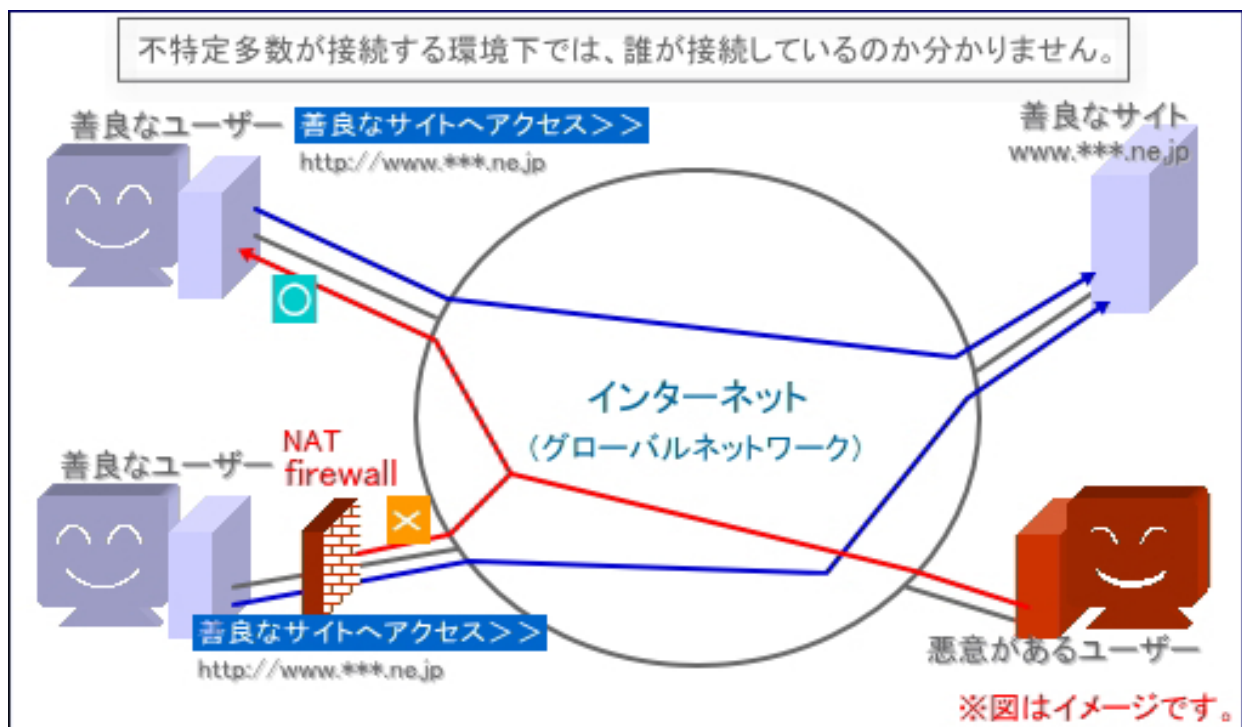
### サービス上の危険性

「ちゅんちゅんネット」のサービスは、インターネット接続に際し<sup>ディジーピー アイピー</sup>TCP/IPプロトコルを使用します。IPの形態は、<sup>どうてき</sup>動的グローバルIPアドレスとなり、セキュリティには十分に注意が必要となります。グローバルIPアドレスは<sup>アイアナ</sup>IANAによって一括管理されており、日本では主に<sup>ジェイピーニック</sup>JPNICにより、各プロバイダー業務を行う業者(<sup>アイエスビー</sup>ISP)に重複しないユニークなIPアドレスが割り当てられます。

IPアドレスの形態には、グローバルIPアドレスともう一つプライベートIPアドレスの2種で成立っています。プライベートIPアドレスとは<sup>ナット</sup>NATなどと呼ばれる機能によって、主にグローバルIPアドレスが変換されたアドレスの事を言います。この違いを簡潔に申しますと、インターネット上からみて、グローバルではある程度の特定制ができますが、プライベートでは特定することが非常に困難だとされています。ですが、グローバルでサービスを受けられるものが、プライベートだと受けられないなどといった特徴があり、一概にどちらが良いとも言えません。

よって、グローバルIPアドレスの場合には、インターネット上に自分のパソコンが見えると思っていた方がよいでしょう。何の対策もしない状態ですと、外部からの接続を許してしまう恐れもあります。(外部からの侵入方法については後ほどご紹介致します。)

対策としては、NAT機能や<sup>ファイアウォール</sup>firewall機能を利用する事が有効な手段の一つです。それらの2つの機能を備えた<sup>ルータ</sup>router(一般の電気店や量販店で手に入ります。モデムとrouterとの接続方法は、「接続してみよう」にも記載しております。)を設置、またはパソコン本体にfirewallソフト(最近のウィルス対策ソフトに付属されている場合があります。)の導入や、不要なサービスを停止するといった「自己防衛」が必要だといえます。





# ケーブルインターネット

by ChunChunNet

## のセキュリティ

### 利用上の危険性

#### 内部的危険性

内部的とは主にソフトウェアの部分指します。ソフトウェアでの危険性で考えられるのは、一般的にバグによる**セキュリティホール(セキュリティの穴)**などが代表的です。ソフトは人の手によって作成されますが、作成段階においてソフト作成者は、あらゆる予測をもとに一連の作業にかかわる動作(結果)をたてています。そうした中において、その予測を超えるケースが出た場合、通常ではありえない動作(結果)を出してしまう場合があります。その事をソフトのセキュリティホールと呼んでおり、開いた穴はふさぐ事をしてあげないと直りません。

これらセキュリティホールの存在は、一般的にインターネットを利用するにあたり必ず必要な<sup>オーエス</sup>OS、サイトを閲覧する時に必要な<sup>ウェブ</sup>Webソフト、メールの送受信に使用する**メールソフト**など、他には、意外に知られていませんが前文で紹介しました**firewall 等機能を有する router**にも存在します。

セキュリティホールがそのままですと、そこから侵入されてしまう事もあり、いくらウイルス対策等のセキュリティ対策を万全に行っても全く無意味となってしまいます。その対策としては、開いている穴をふさぐ「**修正パッチを適用する**」作業を各自にて行わなければなりません。修正パッチは、セキュリティホールが存在するソフトのメーカーのサイト上などで公開しており、ダウンロードできるようになっています。OS であるWindows<sup>ウィンドウズ</sup>で例えますと、「Windows <sup>アップデート</sup>Update 1」と呼ばれるものがそれに該当します。

1 Windows Update によって、ご利用のソフトが正常に作動しない場合があります。それらは、ご利用の環境によって異なりますので、Windows Update は「自己責任(義務ではなく任意)」のもと行って下さい。

OS のセキュリティホールを悪用して、外部から侵入されたケースの代表的な例でいいますと、2003 年頃にネットワークに蔓延した「<sup>エムエス</sup>MSブラスト」と呼ばれるウイルスがありました。このウイルスは、ある OS のセキュリティホールを悪用したもので、OS の修正パッチを適用するといった自己対策を行ってれば未然に防げたのです。結果は、ほとんどの方が対策を行っておらず、ウイルスを削除するのに専門業者に依頼するといった不要な出費を出す結果となってしまいました。

又、ほとんどのソフトウェアは、誰でも使用しやすいように**デフォルト(初期)時の設定はセキュリティに弱い設定**となっています。分かりやすい例でいいますと、Windows Update などのほとんどのデフォルト設定は**自動更新**となっており、意識しないでも更新できるなど一見親切なようにも思えますが、問題はこの自動更新の時間帯にあります。自動更新の時間帯は、「夜中 2~3 時」となっているのが主流です。これではパソコンの電源を一日中入れておく必要があります。一日中電源を入れない方は、この自動更新の時間帯を自分が使う時間帯などに変更の設定をしなければなりません。

どんなに**便利な機能もご利用の環境などの違いによっては何も意味を成さないもの**となってしまいます。環境に応じた設定(カスタマイズ)を行う事が必要なのです。





# ケーブルインターネット

by ChunChunNet

## のセキュリティ

### 外部的危険性

外部にあたるハードウェアでの危険性は、「故障」「盗難」などによるデータ紛失などがあります。「故障」については、「機械だから仕方ない」でもよいのですが、大事なデータを失わない為に**定期的にバックアップ**するといった事で未然に対策ができる訳です。

案外見落としやすいところで、「盗難」があります。顧客の名簿等が保存されたパソコンを使用していて、インターネット上での外からの堅固な侵入対策の firewall などで対策していたが、「盗難」によって内部の蓄積された個人情報が簡単に収集されてしまえば、堅固な侵入対策も何の役にも立たなくなってしまいます。そうした被害を避ける為には、パソコンにログインする**アカウント (特に管理者権限のアカウント)** に**パスワード (誕生日や電話番号など短く単調なものは避ける)**を設定する事も対策としては有効的です。

### 二次的危険性

最近のウイルス感染に関する報告事例で増えてきているのが、「**子供がインターネットを利用して...**」という事例です。**ウイルス感染などの危険性においては、向こうから仕掛けてくるものばかりではありません。あらかじめ不正なプログラムをサイトやソフトなどに用意しておき、それらを興味本位で訪問、ダウンロードさせようとする。**そのほとんどは、視覚的な違和感などありませんから、訪れた本人は気づかない内にウイルスに感染してしまいます。

そういったほとんどのサイトやソフトは、**アダルト系、出会い系などの子供にとっては有害な情報**などに含まれており、その情報の大半が人の心理を利用した**(興味を惹くもの)**といったものです。特に子供は何にでも興味を持つ世代、世の中の善悪の判断は今から社会を通じて学んでいく世代です。そういった環境下においてその被害は増える一方となるのです。また、これらによって感染した場合、被害者だけでとどまらず、**気づかぬ内に同じような被害者を増やす加害者になっている**ことも少なくありません。

それに対する予防策としては、今まで述べてきた対策の実施やウイルス対策ソフト、**フィルタリングソフト**の導入などです。ウイルス対策ソフトは、日々変化するウイルスに対応する為に、そのソフトメーカーから提供される定義ファイルが新しいものでないと検知や削除もできない場合もあります。ただ導入しただけでなく、常に**最新の定義ファイル**に更新する持続性が必要となります。

しかし、近年においてウイルスは、日々新たな種類やその亜種(特徴は似ているが少し変化を加えたものの事)などが発見されている為、そのすべての種類に対しソフトが追いついていない状況もあります。そうした中、一番有効的で持続できる予防策は、怪しいサイトや見覚えのないサイトなどに**興味本位では行かない事**です。その事を使用する本人が十分に理解し、お子さんをお持ちの方はその子供達にその情報を的確に伝えていく、日常のコミュニケーションの場などを通じ、社会のお手本として指導していく立場であることを認識することだと思えます。

危険性を考えれば、皆さんの身近に沢山あります。それら全てはここでは書ききれないほどになってしまいますので、主となる部分だけを紹介致しました。インターネットを利用するにあたって「**100%安全**」**だという事はない**と認知して頂く事がとても重要な事なのです。様々な異なる環境下において、ご利用になる本人がこれらの危険性をどのように理解し、その対策をどのように実施していくかによって、限りなく安全に近づける一番の近道になるものだと考えています。



# ケーブルインターネット

by ChunChunNet

## のセキュリティ

### 様々な侵入方法

インターネットを通じ悪意ある行為を行う者を、一般的に**ハッカー**や**クラッカー**などと呼ばれています。ハッカーは、本来別の意味を持っており、その中のすべてが悪意を持った人だけでないのですが、いつの間にか、ハッカー = 侵入者というイメージが定着してしまっているようです。ここでは、何らかの手法を用いて侵入し悪行を行う人をクラッカーとさせていただきます。

通常、クラッカーと呼ばれる人達は、一体どのようにして侵入を試みるのでしょうか？その手法は、年々複雑さを増していますが、**何らかの経路を経て不正アクセスを試みる**事は確かです。経路で代表的なものが、記憶媒体(フロッピー、CD等)、ツール、メール、ホームページ上などです。又、電子的な経路だけでなく、**ソーシャルエンジニアリング**と呼ばれる手法を用いる事もあります。これらの経路を利用し、何らかの手法で侵入してきます。手法は複数あり、すべてをここでは記載できませんので主な手法を一部紹介致します。

ディー・オー・エス

#### D o S (サービス使用不能攻撃)

Denial of Service の略で、特定のサービス、ホスト、ネットワークなどに攻撃する行為をいいます。攻撃を受けた場合、そのサービスなどが一時的若しくは断続的に使用不能に陥ったりします。他にも分散型(DDoS)などがあります。

#### バッファ・オーバーフロー

規定以上のデータサイズを送りつけ、システムなどの機器を異常な状態にする事をいいます。場合によっては、管理者権限を奪取される可能性もあり、比較的セキュリティホールなどが対象となるケースが多いようです。

#### トロイの木馬

利用者からみて善意のプログラムのように見せかけ、実行したとたんにシステム情報を取得し、外部へ送信したり、バックドアなどを作成して遠隔操作など可能にしたりと、最悪の場合システムを破壊する悪意のあるプログラムです。

#### バックドア

何らかの手法を用いてシステムに侵入した後、再度侵入しやすいように入口(裏口)を作成する行為をいいます。特定のポートを開き「待ち」の状態にし、外部との接続を行います。開いたポートは他の人も利用できてしまうので、ウィルスが侵入される危険性もあります。

#### スパイウェア

アドウェア(画面上に強制的に広告を表示やアクセス履歴などの情報収集を行う)等ソフトを用いて、利用者が意図しない情報を収集する行為をいいます。利用者は知らない内に若しくは、同意画面等をクリックするだけでソフトがインストールされてしまいます。

#### パスワード憶測(なりすまし)

何らかの手法(ツール、辞書等)を用いて他人のパスワードを解析し、取得したパスワードを用いて、いかにも本人であるかのようになりすまします。ニュース事例では、会員制のサイトに友達が自分のIDやパスワードを用いて買い物をしていたという事件がありました。

#### スパム SPAMメール

不特定多数に対し、送られる迷惑メールをいい、近年では、これを利用したフィッシング詐欺による被害も数多くありました。興味を引く内容にアドレスを記載して、訪問者が興味本位で訪れるといった手法です。

#### ボット

上記の手法やセキュリティホールを利用、PtoP(ファイル交換)ソフトの利用、メッセージサービスの利用等によって感染し、感染したパソコンの遠隔操作を目的とした悪意あるプログラムです。感染したパソコンは、外部からの指示を待ち、与えられた指示によって処理を実行します。この動作がロボットに似ている事が由来です。感染した事にはほとんど気づきませんので、近年、このボットに感染したネットワーク(**ボットネットワーク**)が非常に蔓延し問題となっています。

これらすべてを防ぐ事は容易ではありません。防ぐ事はできなくても、不要なものは極力省くといったそれぞれの環境に応じた予防・対策は簡単にできます。まずは、使用しない時はネットワークから切り離す事から始めてみましょう。

ツールなどはネット上で簡単に入手でき、誰でも簡単に操作できる為、一歩間違えると「加害者」になりかねません。決して「加害者」にならないように「人としてのモラル」を守り、秩序ある正しい利用をされて下さい。



# ケーブルインターネット

by ChunChunNet

## のセキュリティ

### 被害対策

もし、自分が不正アクセスやウィルス感染の「被害者」となってしまった場合どうすればいいのでしょうか？不正アクセス等における被害にあった時は何をすればよいものか、全く検討もつかないのがほとんどだと思います。又、被害者となるケースは不正アクセスやウィルスだけではなく、ネット犯罪やその他詐欺行為などインターネットを利用する環境では様々なケースが考えられます。

ここでは、そういった時の相談窓口や、情報を提供している機関を紹介致しますので、ご参考にされて是非ご活用下さい。

#### セキュリティに関する被害報告や再発防止技術情報

情報提供： 有限責任中間法人(JPCERT) <http://www.jpCERT.or.jp/>

#### ウィルス情報の提供や対策情報

情報提供： IPA 独立行政法人 情報処理推進機構 <http://www.ipa.go.jp/security/index.html>

インターネット セキュリティ ナレッジ <http://is702.jp/>

Cyber Clean Center 総務省・経済産業省 連携プロジェクト(ボット情報) <https://www.ccc.go.jp/>

#### ハイテク犯罪(改ざん、詐欺行為、不正アクセスなど)に関する情報

相談窓口： 佐賀県警察本部警備第二課 <http://www.saganet.ne.jp/kenkei/osirase/internet/internet.html>

#### 架空請求や悪徳商法、その他 SPAM メールに関する情報

相談窓口： 地方公共消費者センター <http://www.saganet.ne.jp/kenkei/osirase/internet/internet.html>

この資料に関するお問合せ先

西海テレビ株式会社 〒849-4256 佐賀県伊万里市山代町久原 2994 番地 5

TEL:0955 - 28 - 2466 FAX:0955 - 28 - 1650 E-Mail:sky-catv@po.chun2.ne.jp / info@po.chun2.ne.jp

ホームページ: <http://www.chun2.ne.jp/>





# ケーブルインターネット

by ChunChunNet

## のセキュリティ

### 用語解説

#### ・TCP/IP ティ・シー・ピー アイ・ピー プロトコル

Transmission Control Protocol/Internet Protocol の略で、プロトコルはインターネット上での通信を行う際に、異なるデバイスやコンピュータのデータのやり取りを正常に処理する為に規定されてものをいいます。TCP/IP は、現在もっとも広く普及しているプロトコルの一種で、TCPは信頼性があるプロトコルであり、IPによって経路を知ります。今では必要不可欠なものであり、基本的なプロトコルといえます。その他UDPやICMPなどがあります。

#### ・IP アイ・ピー

Internet Protocol の略で、インターネットでのパケットの宛先や送信先にあたる部分です。8ビット列区切りの4つで構成されており、この情報を基に正常な通信が確立されています。

#### ・動的 どうてき

一定の期間において変化するもので、対義語では静的にあたります。

#### ・グローバル

インターネットの世界において、公式に割当てられたものであり、世界的にユニークな(重複しない)構成になっています。

#### ・IANA アイアナ

Internet Assigned Numbers Authority の略で、インターネットにおいて、名前や番号の登録を必要とする情報の登録業務を行う組織の事。

#### ・JPNIC ジェイビーニック

JaPan Network Information Center の略で、設立当初から JP ドメイン名登録・管理や日本における IP アドレスの割り振りなどを中心として行っている。国内基盤整備を中心とした IP アドレス事業、ドメイン名関連事業、インターネットに関わる調査、研究や教育活動を行うインターネット基盤事業を行っている。

#### ・プライベート

内面的な意味を持つもので、インターネットの世界では定められた IP の範囲があります。

#### ・NAT ナット

Network Address Translation の略で、一つの IP アドレスを複数のプライベートな IP アドレスに変換する技術で、限られた IP アドレスを有効活用する目的で構成されました。この機能を拡張されたものを NATP(又は IP マスカレード)と呼びます。

#### ・firewall ファイアウォール

防護壁の意味を持ち、外部からの侵入などを制限する機能を指すもの。パケットフィルタリング等を用いてアプリケーションの制限を行います。

#### ・router ルーター

複数のLAN(Local Area Network の略)同士や LAN と WAN(Wide Area Network)を接続し、通信を可能にする機器のことです。一般的に複数のパソコンでインターネット接続する場合に用いられる事が多い。又、市販されている物でも簡単な NAT 機能や firewall 機能などを有したものもあります。

#### ・OS オーエス

Operating System 略で、一般的に普及している OS が Windows であり、その他MacintoshやUNIX系などがそれにあたります。他のアプリケーションソフト(特定の操作をする為のソフト)を操作するのに必要不可欠なソフトウェアです。

#### ・アカウント

パソコンやソフトなどにアクセスする際のアクセス資格となるログインアカウントの事をいいます。





### 用語解説

---

#### ・管理者権限のアカウント

Windows 環境においてデフォルトは、Administrator(アドミニストレータ)がそれに該当するアカウントで、資源の管理・構成の変更などを行う際に必要なアカウントの事をいいます。他には root(ルート)などがあります。

#### ・フィルタリングソフト

主として、子供達にとって有害となる情報を見せないよう、意図的にブロックかける目的としたソフトです。子供にとって有害となる情報のアダルト系や出会い系などを表示させないようし、無害な情報は見るできるように制限を掛けます。このソフトは、ウイルス対策ソフトに付属されている場合や又は、単体のソフトとしても販売されています。

#### ・不正アクセス

ID(アカウントなど)やパスワードの不正使用、アクセス権限がないコンピュータ資源などのへの何らかの手法を用いてアクセスする行為をいいます。これらに関する定義や違反した場合の罰則などの取り決めが、法律(不正アクセス禁止法)によって定められています。

#### ・ソーシャルエンジニアリング

システム管理者や利用者とは何かの手法で接触し、情報(パスワード、ID 等)を入手する行為をいいます。会社から出たゴミなどから情報を入手、ログイン画面でパスワードを入力中に覗き見るといった方法も利用するケースもあります。又、社員から聞き出す事もあり、個人情報の流出は、それらケースを含めた内部から要因が7割近くといわれています。