第３章

パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使おう

私たちの、安全なインターネット生活を支えるパスワード、Wi-Fi(無線LAN)・ウェブ・メール。
それらを安全に利用したり、その内容を盗聴や流出から守る暗号化など、
セキュリティについての理解を深めましょう。
初心者向けとしてはやや難しい項目ですが、なるべく平易な言葉で解説していきますので、
ぜひ読んで、セキュリティへの理解を深めてください。

1 パスワードを守る、パスワードで守る

1 パスワードってなに？

私たちが、スマホやパソコンなどのIT機器や、各種のウェブサービスを使う上で、欠かせないのが「パスワード」です。

機器やウェブサービスを利用するときに、正当な利用者や持ち主である自分だけが利用でき、他人が利用できないようにするための鍵の役割を果たすものです。

パスワードは、いわば「家の鍵」や「金庫の鍵」。これを適切に守らなければ、家や車、金庫を勝手に開けられてしまうように、パソコンやスマホ、ウェブサービス上にある私たちの個人情報やメール、銀行口座が攻撃者に不正にアクセスされ、情報が流出したり、お金を盗まれたりしてしまいます。

なお、こういった役割を担うものには、ほかに「暗証番号」などや、通信している情報やパソコン・スマホの中のデータを暗号化して、他人や攻撃者が読めないようにする、「暗号化と復号の鍵＝暗号キー」というものもあります。

この3つは、性格や役割が異なるのですが、よくまとめて「パスワード」と記述されることがあるのと、暗証番号、パスワードと暗号キーは、等しく攻撃の対象になるために、ここでは一括して扱います。

2 3種類の「パスワード」を理解する

私たちは、機器やウェブサービスを利用するとき、あるいはファイルを開くときに入力するものを、まとめて「パスワード」と呼び、同じような役割をするものと思いがちです。しかし、セキュリティ上の性質から、「パスワード」とまとめて呼ばれるものは、大きく3つに分けて理解する必要があります。

1. 銀行のキャッシュカードやクレジットカードの利用時や、スマホのロック解除時に使用し、通常4桁から6桁以上の数字だけで構成されることが多いもの（暗証番号やPIN、PINコード、パスコード。通信事業者のネットワーク暗証番号などを含む）

2. パソコンやデジタル機器、ウェブサービスなどの利用時にIDとセットで入力し、英大文字小文字、数字、記号を用い複雑さと一定以上の長さが推奨されるもの（狭い意味でのパスワード、ログインパスワード）

3. パスワードと呼ばれていることもあるけれど、本当はファイルや通信内容を暗号化しまた復号するための暗号鍵として使われているもの（ZIPファイルのパスワード、WordやExcel、PowerPointの保護パスワード、Wi-Fi機器の暗号化キー、暗号キー、パスフレーズ、セキュリティキー、ネットワークキー）

一口にパスワードといっても、上記のとおり、実に様々なものがあります。P30でご紹介したのは、上記のうちの2にあたります。

この本では、以降、この3つを混同しないように、

1を「PINコード」
2を「ログインパスワード」
3を「暗号キー」

と呼びます。

3 「PINコード」と「ログインパスワード」に求められる複雑さの違い

P30では、機器やウェブサービスを利用するとき、「ログインパスワード」として、英大文字小文字＋数字＋記号混じりで少なくとも10桁以上を推奨しました。

一方、同様に使う「PINコード」は、メーカーが数字のみの4桁から6桁以上で良いとしています。

この2つは、両方とも機器やウェブサービスを利用するときに使用するのに、求められる長さや複雑さに差があるのはなぜでしょうか。

そもそもパスワードに「複雑さ」が求められる理由は、攻撃者が制限のない状態でパスワードの文字列を総当たりで試すと、時間はかかるが「いつか必ず探り当てることが可能」だからです。これは、どんな複雑な「ログインパスワード」でも変わりません。

こうやって力業（ちからわざ）でパスワードを探り当てる攻撃を「総当たり攻撃（ブルートフォース攻撃）」と呼びます。「ログインパスワード」を守る第一歩は、いかにこれを成功させないかにあります。

スマホの「PIN コード」の場合は、数回間違うと「入力遅延」といって一定時間「PIN コード」を入力できないようになり、さらに「10 回間違えば以降 PIN コード入力不可にする（ロック）」「場合によっては機器を初期化する（ワイプ）」ことで「総当たり攻撃」を不可能にし、攻撃者による不正利用を防ぎます。

さらに、厳しいキャッシュカードなどでは、3回間違うと以降カードが利用できなくなりますが、これも同じ考え方です。

「PIN コード」では、こういった厳しい制限を設けることで「総当たり攻撃」を不可能にし、4桁から6桁以上の数字でも攻撃者から機器やサービスを守れるのです。

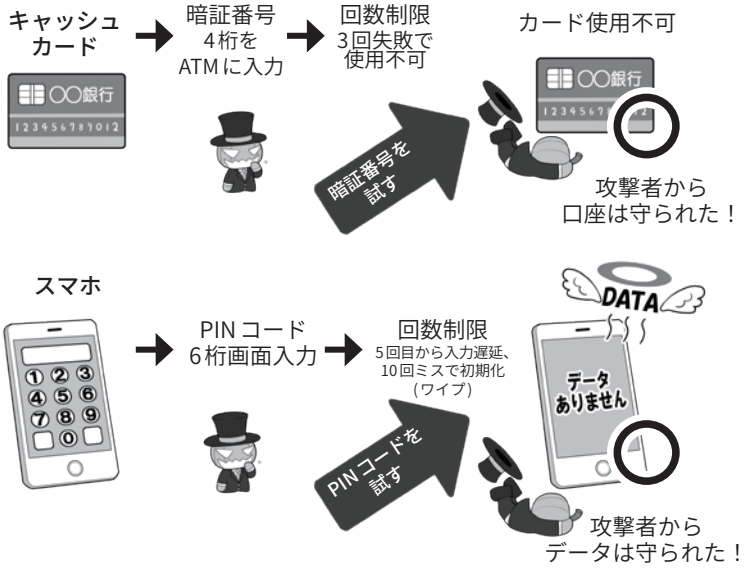
一方、「ログインパスワード」は、通常「PIN コード」のようにワイプまでする機能がついていることはほぼありません。数回失敗すると入力間隔が開く、一定時間入力をロックするなどのペナルティを受ける場合もありますが、ペナルティがないものも多いのです。

この「ログインパスワード」は、ウェブサービスのログインページや、パソコンや IoT 機器のログイン画面に入力するもので、こういった入力画面では、ネット経由でログインを試みた場合、どう頑張っても1秒に数回〜数十回程度しか入力することができず、これだけで実質的に高速な攻撃を防ぎます。

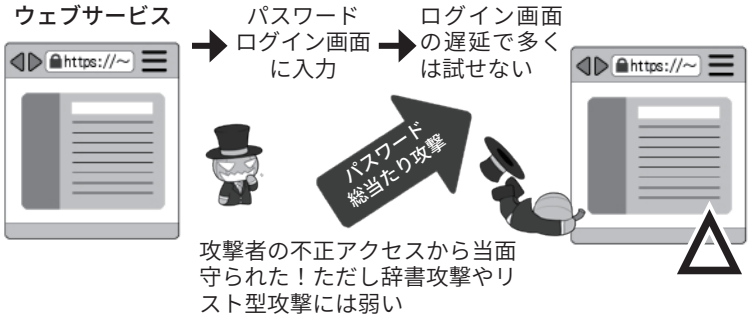
本書の推奨どおり、英大文字小文字＋数字＋記号 26 種＝88 種類の文字を使い、10桁のパスワードを作ったとすると、その組み合わせは約2785 京個（京は兆の上の単位）、1秒5回の制限で「総当たり攻撃」をした場合、全部を試すまでに約1760億年かかるわけです。

3種のパスワードを理解する

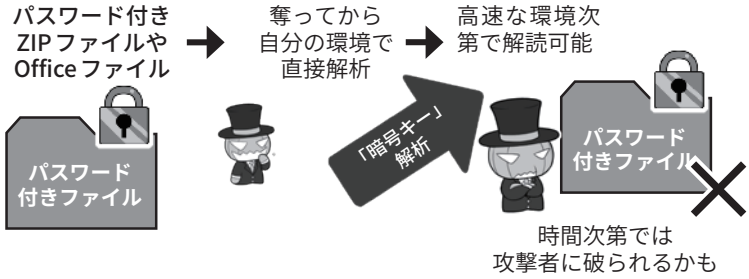
①「PIN コード」の例



②「ログインパスワード」の例



③「暗号キー」の例

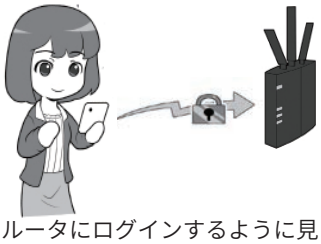


わかりにくい例

「ログインパスワード」か「暗号キー」か分からない例

暗号化された記憶装置 (ハードディスクや SSD) の救済に関して、「ログインパスワード」なのか「暗号キー」なのか分からないものを求められたら「暗号キー」と考えましょう。

無線 LAN アクセス時にパスワードのように入力する文字列



ルータにログインするように見えますが、ログインパスワードではありません。「暗号キー」を自分の機器に設定しているだけなので、「暗号キー」の基準で設定します。

※この図は一例であり、実際の機器の条件とは異なります。

これならば、100年以内に探り当てられる確率は非常に小さく、事実上不可能といえるわけです。

このような攻撃の想定を、セキュリティ用語的には「オンラインアタック(攻撃)」といいますが、ここでは「『ログインパスワード』への攻撃」と呼ぶことにします。

4 「暗号キー」に求められる複雑さ

上記の「ログイン画面」に入力する「ログインパスワード」とは異なり、「暗号キー」の場合は、攻撃者が暗号化されたデータを盗んで持ち帰り、ログイン画面の遅延などなく、自分のペースで暗号化解除(解読)の高速攻撃ができます。

この攻撃の対象となるのは、「複数のファイルをまとめたパスワード付きZIPファイル」、「パスワードを設定したMicrosoft Officeのファイル」、「暗号化されたUSBメモリ」や「パソコンから取り出された内蔵補助記憶装置(ハードディスクやSSD。以下記憶装置)」、あるいは「暗号化された無線LAN通信の内容」などです。

こういったものでは、「パスワード」と思って設定しているものが、実はパスワードではなく、中身を読まれないようにするための暗号化に使われる鍵=「暗号キー」となっている場合が多いのです。

ZIPやMicrosoft Officeのファイルは、パスワードが設定されていると、開くときにパスワード入力画面が出るので、入力遅延の防御があるように見えますが、実はその画面はZIPやOfficeのプログラムが提供しているもので、ファイルそのものは単なる暗号化されたデータにすぎないのです。

そのため、パスワード入力画面を使わなくても直接ファイルに対して暗号化解除の攻撃が可能であり、遅延による防御はありません。

このような暗号化解除は、「暗号キー」が短いと、スーパーコンピュータを使うまでもなく、普通に市販されているゲーム用パソコンの性能で十分可能です。そういったパソコンの、グラフィックボードに搭載されているGPUというプロセッサーを駆使すれば、ZIPファイルに対して40億回/秒の暗号化解除の攻撃が可能というデータすらあります。

この場合、先ほどの約2785京個の組み合わせがある場合でも、解読までにかかる期間は78.5万年に短縮、8桁のものになると103年、8桁で記号抜きの62種の文字だと6年、英大文字小文字だけだと2年となり、GPUの性能が向上すればそのうち、数日単位で可能になるでしょう。それは、もう「解読可能な領域」といえます。

そのため本書では、「暗号キー」には、完全にランダムで英大文字小文字＋数字＋記号混じりで15桁以上のものを推奨し、これを基準とします。

ZIPのパスワードに、15桁ものランダムな文字列を使うのは、覚えられなくて無理だと思われるでしょうが、8桁程度のパスワードでは破られてしまうので、暗号化したつもりでも攻撃者の前では意味がないのです。

なお、このような想定の攻撃をセキュリティ用語的には「オフラインアタック(攻撃)」と呼びますが、ここでは「『暗号キー』への攻撃」と呼ぶことにします。

5 総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御

パスワードなどを破る攻撃には、「総当たり攻撃」のほかにも様々な手法があります。

パスワードでよく使われる言葉などを集めた、専用の辞書を利用する「辞書攻撃(ディクショナリアタック)」、ウェブサービスなどから流出した名簿やIDとパスワードのリストを入力して試す「リスト型攻撃(アカウントリスト攻撃・パスワードリスト攻撃)」など。

これらに対する防御のためにも、「ログインパスワード」には意味のある単語や、自分に関連の深い語句やよく使われるパスワードは避け、推奨する基準に従い、充分に複雑で、かつほかの機器やウェブサービスで使い回していないものを設定しましょう。

「PINコード」は、入力を間違え続けると「入力遅延」や「ロック」機能があるため、「総当たり攻撃」などの手法が有効ではありません。

しかし、「PINコード」の強さは「盗み見や、推測されないこと」が前提ですので、入力するときは周りに気を配り、また、自分の個人情報など推測しやすいものは使わないようにしましょう。

現に、ATMでお金を下ろすときに、「暗証番号(PINコード)」を肩越しに覗き盗み取る手口は、「ショルダーハッキング」としてよく知られています。

「PINコード」の盗み見などを防ぐためには、指紋認証や顔認証などの「生体認証」を利用するのも一つの手です。それらなら肩越しに見られても、攻撃者が容易にまね

をすることはできないからです。

ただ、指紋認証などの生体認証も100%安全とはいい切れません。最近では、どこかで撮影した相手の指の写真から、3Dプリンターで偽の指紋を作って認証を突破したり、顔を印刷した紙を加工して、それを使って顔認証を突破したりする実験も行われています。

また、指紋認証が携帯電話に登場したときから、本人が寝ている間に、勝手に指を押し当てて認証を突破するという話があります。最近では、親が寝ている間に子どもが勝手に認証し、ゲームに課金していたという例もありました。

したがって、勝手に認証される可能性がある環境では、「PINコード」入力が必要になるよう、わざと生体認証を数回失敗させて、それ以上勝手に生体認証できない状態にするなどの工夫が必要です。

生体認証はこのほかにも、目の虹彩の模様によって認証する「虹彩認証」、手や指の静脈のパターンで認識する「静脈認証」などがあり日々進化しています。それぞれの特徴やセキュリティ上のメリットをよく検討して利用しましょう。

「暗号キー」は、攻撃に遅延がないので、「総当たり攻撃」を含めすべての攻撃が有効です。また、攻撃されるまでもなく、そもそも「暗号キー」が漏れていれば暗号化された中身が解読され、ひとたまりもありません。この暗号キーが、事実上漏れた状態になる話は、P64以降で詳しく説明します。

パスワードを破る手段は色々

総当たり攻撃（ブルートフォース攻撃）

すべての文字列の組み合わせを試す

リスト型攻撃（アカウントリスト/パスワードリスト攻撃）

名前やIDとパスワードの流出リストを使う

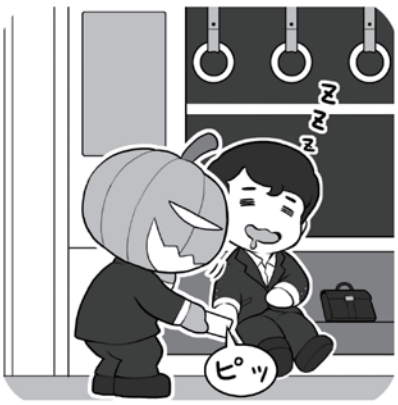
辞書攻撃（ディクショナリアタック）

パスワードでよく使われる単語を使って試す

あくまでも代表的なものの例ですが、簡単なパスワードやよく使われるパスワードだったり、使い回しをしていたり、流出したのに放置していると、攻撃者に楽々突破されます。パスワードはしっかり管理しましょう。

（本当は、図のように人力ではなくプログラムなどで自動的に行われます）

指紋認証が破られることも…



高度なハッキングをしなくても、酔っ払って寝ているあなたの指に押し当てるだけで指紋認証は突破できてしまいます。

指紋認証だから、絶対安心と過信しないようにしましょう。

場合によっては、機器を再起動したり、わざと数回指紋認証を失敗して、強制的にPINコード入力が必要な状態にしましょう。

6 多要素認証を活用する。ただしSMS認証は避ける

IDとパスワードでの認証に、さらにチェック機能を追加するのが二要素認証以上の多要素認証と呼ばれる機能です。これを利用することで、パスワード流出時の乗っ取りをより困難にします。

もっとも一般的なものは、なんらかの手段で入手する、その場限りの「ワンタイムパスワード」の入力を追加する方法です。

ログインに当たって、サービス提供者から、SMS（ショートメッセージ）や電子メールで送られてくるものを利用する方法や、スマホのアプリを使って生成するソフトウェアトークンや専用の小さな乱数を発生するハードウェアトークンを利用する方法、そして物理的なUSBセキュリティキーや生体認証を用いる方法があります。

このうち、SMS方式は海外で乗っ取りからの成りすましで破られた例があり、電子メールも経路上で奪取される可能性があるので、自分で種類を選択できる場合は、トークン、USBセキュリティキー、または生体認証を推奨します。

ソフトウェアトークンは、専用のアプリを利用するものと、QRコードを使って情報を読み込むものがあり、後者はパスワード管理アプリで一括して管理できる場合もあるので、活用しましょう。

スマートウォッチによっては、スマホのパスワード管理アプリと連携して、手元でIDとパスワードを確認したり、ワンタイムパスワードを発生させたりできるので、より快適なパスワード管理を求めるならば活用しましょう。

また、パスワードをネット経由で送信しない方式の採用も推進されています。より安全な利用のために、アンテナ高く情報収集しましょう。

7 二段階認証と二要素認証と多要素認証の安全性

ウェブサービスのアカウント乗っ取りを防ぐための追加の認証。

この認証のために用いる要素には下図にあるように、「知っていること」「持っているもの」「本人自身の一部」などの種類があり、このうち最初の認証に用いなかった要素と組み合わせて、二要素以上を用いた認証方式を構成することが重要です。

この要素を、二つ用いて行うものを二要素認証、それ以上に用いて行うものを多要素認証などと呼びます。

本冊子では、その意味で推奨する認証方式を「二要素以上の多要素認証」という表現をします。

一方、アカウント認証に関する記事等でよく用いられる言葉に「二段階認証」というものがあります。これは、認証のプロセスを二段階に分けて行うものであり、構成する要素とは関係がありません。

従って、二段階認証であっても一要素認証もあれば、一段階認証であっても二要素認証の場合もあり、前者よりは後者の方が安全性が高まります。

また要素のうち、「持っているもの」「本人自身の一部」は、物理的な存在であるため、例えば攻撃者がこれを突破しようとすると、物理世界で窃盗や脅迫を行わなければならず、ネットの影に隠れたまま行える犯罪よりもリスクが高くなり、安全性が高まります。

それでも、「知っていること」と「持っているもの」の組み合わせであるキャッシュカードが、オレオレ詐欺などであっさり奪われたり、P76に解説しますが、多要素認証すら破る「中間者攻撃」も存在したりするため、多要素認証だからそれだけ絶対安全と思い込まないで下さい。

常に「自分は、狙われているかもしれない」「攻撃されているかもしれない」「もしかしたら、これは攻撃かもしれない」という危機意識を持つようにして下さい。

現時点で推奨できる多要素認証要素

基本的に推奨できるもの

ソフトウェアトークン
（ワンタイムパスワード生成）

USB
セキュリティ
キー

生体認証
（指紋認証など）

アプリから認証

推奨できないもの

SMS（ショートメッセージ）や
メールでワンタイムパスワード送信

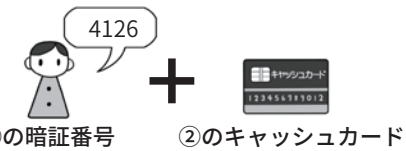
SMSを使ったワンタイムパスワード受信は、海外でSIMハイジャックという攻撃により破られた例があります。また、メールも同様にパスワードを「送信する」をいう点で攻撃の余地が多くなります。

多要素認証の構成要素は？

①知っているもの　②持っているもの　③本人自身に関するもの

多要素認証の組み合わせ例

銀行のキャッシュカードの例



①の暗証番号　＋　②のキャッシュカード

スマホからウェブサービスへ
ログインする例

②のスマホの固有情報　＋　③の指紋情報

8 パスワードの定期変更は基本は必要なし。ただし流出時は速やかに変更する

利用するサービスによっては、パスワードを定期的に変更することを求められることがあります。しかし、前出のように十分に複雑で使い回しのないパスワードを設定し、実際にパスワードを破られアカウントを乗っ取られたり、サービス側から流出したりした事実がないのならば、基本的にパスワードを変更する必要はありません。

むしろ、パスワードの基準を定めず、定期的な変更のみを要求することで、パスワードが単純化したり、ワンパターン化したり、サービス間で使い回しするようになることの方が問題となります。

ただし、アカウントが乗っ取られたり、流出の事実を知った場合は速やかにパスワードを変更し、その原因も特定しましょう。

原因が、マルウェアなどでパソコン側から情報が流出し続けている場合、その穴を解明しないまま放置していると、パスワードを変更しても意味がありません。

また、アカウントが完全に乗っ取られてしまったら、ウェブサービスに連絡して復旧しましょう。

一方、自分の使用機器からではなく、ウェブサービスなどの側からパスワード流出が起きた場合は、速やかにパスワードを変更の上、流出の原因となった点の対策が行われたかを確認しましょう。

サービス側からパスワード強制リセットの通知や、再設定のリクエストが来たら、次項の便乗攻撃に注意しつつ、同様に速やかにパスワードを変更しましょう。

9 パスワード流出時の便乗攻撃に注意

サービス側から、パスワード再設定の通知がメールなどで送られて来た場合、まずそれが本当にサービス側から送られてきたものかどうか、該当のサービスのウェブサイトやニュースサイトでチェックし、事実の確認をしましょう。

サービス側を装ったパスワードリセットの通知は、流出事故に便乗したフィッシング詐欺などのよくある攻撃パターンです。パスワードを奪う攻撃者の罠かもしれません。通知のメールにパスワードリセットのリンクなどが貼られていても、うかつにクリックしたりせず、リセットする場合も直接公式サイトやアプリからしましょう。

なお、ウェブサービスを利用するときは、パスワードが流出した場合に簡単にアカウントを乗っ取られないように、必ず二要素以上の多要素認証を設定しておきましょう。これが提供されないサービスは、セキュリティ意識が低いと言えるので利用は再考しましょう。

10 適切なパスワードの保管

さて、日常的にインターネットを利用していると、IDとパスワードは無限に増えていきます。どう管理すればいいのでしょう。

本書では、「スマホ用のパスワード管理アプリ」か「物理的な紙のノート」の利用を推奨します。

スマホのパスワード管理アプリを導入する場合は、ネットにデータを置く「クラウド連携（バックアップ）機能」を安易に利用せず、まずはスマホ内だけで管理する「スタンドアロン」状態で利用できる

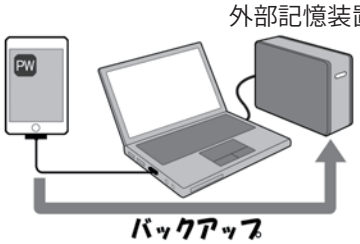
ウェブブラウザにはパスワードを保存しない

ウェブブラウザにパスワードを保存すると、席を離れたときに勝手に利用されたり、パソコンをクラッキングされた際に根こそぎ盗まれる可能性があります。

パスワード管理方法の例

一見分かりにくい専用の紙のノートに二重で

管理アプリのデータは、暗号化した外部記憶装置にバックアップ



紙のノートに二重に記入したり、スマホのパスワード管理アプリを使って、パソコン経由で外部記憶装置にバックアップする方法があります。紙のノートは、一見内容が分からないようにできる専用のノートも売られています。

ものを優先しましょう。

紙と比較した場合、スマホはネットに接続されているので、攻撃者にクラッキングされる可能性は捨てきれませんが、利用規約を守り、システムを最新に保っている限りは、スマホのセキュリティは十分に高い設計となっています。

また、紛失や盗難に遭っても、最新のスマホはデータを暗号化した状態で保存していますし、管理アプリも独自に暗号化するので二重に暗号化された金庫での保管に等しくなります。加えてスマホは、事前にきちんと設定しておけば、紛失や盗難に遭っても遠隔操作でロックして操作できなくしたり、場合によってはワイプ(消去)して情報流出を避けたりできるという、紛失に対する三重四重のセキュリティが設けられています。

一方、紙のノートを推奨する理由は、あたりまえではありますが、紙のノートはネットに接続できないからです。接続できなければネット経由のサイバー攻撃も不可能です。奪うには現実世界で「盗む」という行動を起こさなければならず、攻撃者が姿を現すリスクがあることが抑止力になるからです。

11 パスワード情報をクラウドで保管する善し悪し

パスワード管理アプリや、同様の機能を持つソフトには「クラウド連携機能」やクラウドを用いた「バックアップ機能」があり、これを利用すると複数端末でパスワード情報を共有できたり、明示的にバックアップ処理をしなくても自動でクラウド上にバックアップデータが作られたりします。

この機能を無条件で推奨しない理由は、「重要な情報が複数箇所に存在すれば、流出する可能性がその分増える」からです。

加えて、クラウドサービスを利用する場合、他人の手元でデータが保管されますが、利用者には、そのサービスが運用しているシステムのセキュリティレベルの実態を知ることも管理することもできません。

また、パスワード管理アプリのデータがスマホ上にある限りは「PINコード」方式で守られますが、クラウドのバックアップデータが流出すれば、マシンパワーにものをいわせた高速なオフラインアタック、暗号化解除の攻撃が可能になるからです。

銀行の口座からお金が盗まれれば、自分にミスがない限り銀行が補填してくれますが、クラウドから流出した情報は実質的に回収不可能です。これは、「お金は補填が可能だが、重要情報の秘密性は戻らない」からなのです。

パスワード管理方法のメリットデメリット

	利便性	盗まれたときの対策	ネット経由のセキュリティ	データの管理者
紙のノート	△ 持ち歩き可でも落とすと読まれる	× 家にあると盗まれにくいが、盗まれると対応できない	○ 攻撃不可	本人
スマホアプリ	○ ロックしたまま持ち歩き可	○ バックアップがあれば復元可能	△ セキュリティレベルによる	本人
外付けHDDへバックアップ			○ ただし普段は接続しない	本人
クラウドサーバにバックアップ			△ サービス側のセキュリティレベルによる	事業者

パスワードの管理方法とバックアップ方法を、一つの表で同列にまとめていますが、一番右列のデータの管理者の項目をよく見て下さい。クラウドサービスを使ったバックアップは便利ではありますが、データの管理者は自分ではなくなります。また、クラウドサービスのセキュリティがどのレベルなのかは、自分では容易に判断できません。

パスワードに関してのみは多少の不便さはあっても、自らの責任において管理するのか、それとも他人の手を借りるのか、クラウドはそれに伴うメリットとデメリットをよく勘案して利用しましょう。

12 ノートやスマホを失くした場合のリカバリ考察

さて、パスワードを記録したスマホも紙のノートも、紛失してしまうと困るのは同じです。ただ、スマホの場合、パソコンでスマホのデータを丸ごと暗号化してバックアップをしておけば、紛失しても代替機をパソコンに接続し「復

元」を指示するだけで、環境やパスワード管理アプリの内容を含めて、すべて元の状態にできるものもあります。

また、スマホを丸ごとバックアップしなくても、パスワード管理アプリのデータを、パソコン経由で暗号化された外部記憶装置などにバックアップし、普段は接続せず適切に保管しておけば、復旧は容易です。アプリによっては紙に印刷して保管する機能もあります。

なお、クラウドサービスのメリットとデメリットを理解した上で、クラウドを使った複数機種での連携機能、自動バックアップやそれに付随するリカバリ機能を利用するのは一つの選択肢といえます。

紙のノートの場合は、紛失したときに備え2冊同じものを作り、一つは金庫に保管するなどのバックアップ手段を取りましょう。

紙のノートによるパスワード管理は、平文で書いてあるものを持ち歩いて紛失してしまった場合、中を見られないような制限はかけられませんので、一見してもパスワードが分からない、専用のノートを利用するのが安全でしょう。

13 注意するべきソーシャルログイン

機器やウェブサービスのパスワードは、使い回しをしないのが絶対です。しかし、膨大な数のパスワードを暗記するのは非現実的なので、必然的にパスワード管理アプリやパスワード管理のノートを使う必要があります。

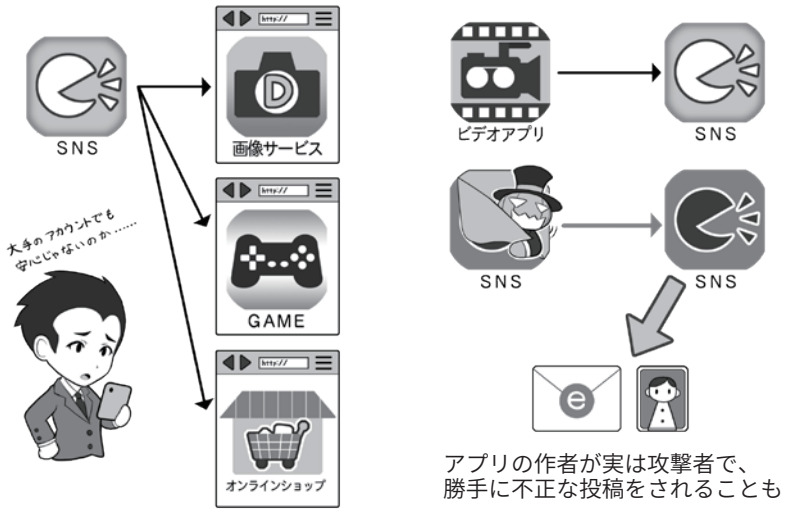
この手間は、情報漏えい対策のために「パソコンのウェブブラウザにIDやパスワードを覚えさせる機能(＝自動入力)」を使わないならなおさらです。

これを解決する策として、「ソーシャルログイン」という方法が用いられて来ました。これは、IDとパスワードの管理がしっかりしたウェブサービスのアカウントで、ほかのウェブサービスにログインして利用するというものです。

しかし2018年時点で、最大手SNSサービスから、ソーシャルログインで用いられる身分証明の証(トークン)が流出するトラブルがあったため、本書では、ソーシャルログインを非推奨として、基本的にそれぞれのサービスは別々のIDとパスワードを設定することのみを推奨することとします。

トークンが流出すると、IDとパスワードが流出しなくても、ソーシャルログインを設定していたサービスに根こそぎアクセスして

ソーシャルログインとサービス・アプリ連携の違い



ソーシャルログインは、堅牢なサービスのアカウントを別のサービスの鍵に使え便利ですが、大本のアカウントの認証情報が漏れる事案が発生したため、それぞれのサービスに別々のパスワードを使用する基本対応を推奨します。

アプリなどの連携は定期的に棚卸ししよう

自分が意識的に連携をしていなくても、ネット経由で回ってきた「面白いアプリ」を利用したら、いつの間にか連携されていたということもあります。また、そのときは問題がなくても更新時に権限の拡張を求めてきて、結果的に個人情報を「合法的に」奪うアプリも存在しています。

アプリ連携やアプリの権限は、定期的に棚卸をして、不必要なものや不審なものは連携解除するか、削除するようにしましょう。

しまえる可能性があるからです。

一方、それぞれのウェブサービスを利用するときに、別々のIDとパスワードを入力する手間を省くために、パスワード管理アプリが進化し、ウェブサービスやアプリのログイン時に、自動的に入力してくれる機能も登場してきました。多要素認証などの使い捨てパスワード入力も楽になっています。

それらを活用し、パスワードの使い回しをせず、ストレスなくルールを守るようにしましょう。

14 権限を与えるサービス連携にも注意

ソーシャルログインと混同されやすいものに、SNSに関する機能で「サービス・アプリ連携」というものがあります。

例えば、AというSNSにBというサービスやアプリから、投稿を認めるといったものです。具体例としては特徴的な機能を持つカメラアプリにSNSへの写真付き投稿を認めるといったものがあります。

これは、ソーシャルログインとは別の性格の機能ですが、ときに「連携するアプリやサービスに投稿を認める(＝権限を与える)」という部分が、攻撃者の手段として利用されることもあるので、利用は避けるようにしましょう。

SNSを利用していると、自分が意識しないうちに誤操作をし、知らずにサービス・アプリ連携していることもあります。

定期的に使用しているSNSアカウントの「連携を確認できる画面」を開いて、知らないアプリや止むを得ず使ったサービス・アプリの連携があれば解除しましょう。

コラム：暗号化の超簡単説明

暗号化とは、自分と相手だけが読めて他人は読めないという、セキュリティを保つ技術です。

暗号化というと非常に難しく感じるかも知れませんが、大丈夫、その心配にはあたりません。

ただ、暗号化の内容を詳しく書くとそれだけで本になってしまうので、ここではその概念だけをごく簡単に説明します。

1．暗号化とは「魔法をかけて手紙などの内容を読めないようにする」ことです。

2．暗号化の魔法にはいくつもの系統(方式)があり、魔法をかけるには呪文(「暗号キー」)を決めて使います。

3．魔法の呪文(「暗号キー」)がばれると、魔法が解けて内容が読めてしまいます。

4．古い系統の魔法の中には、その仕組みに不備があり、呪文が分からなくても解けてしまうものがあります。

初歩としては、このぐらいの理解があれば大丈夫です。

使用する暗号方式が安全かどうかは、魔法研究の専門家に任せましょう。車がどうやって動くのか知らなくても、安全な利用ができるのと同じです。

大切なのは、正しい使用法を知ることと、専門家が「危険が発生した！」という情報を発信したらキャッチし、迅速に避けるように行動することです。

右のイラストでは、具体的に危険が発生する例を描いていますので、是非覚えておいてください。

まず第一歩は、「正しく使うこと」からです。

Cipher Disk(シーザー暗号)

もっとも原始的な暗号は、シーザー暗号といわれるものです。文字をずらして記述するだけのシンプルなもので、仕組みさえ分かればアルファベットなら26回試すまでに暗号が解けてしまいます。

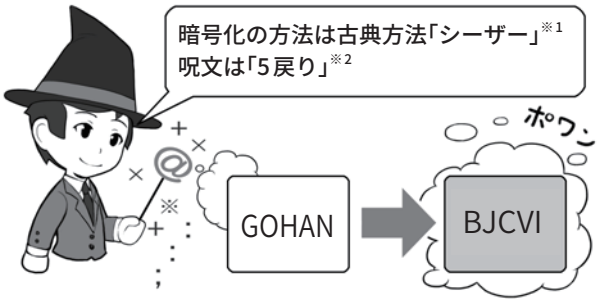
上の図は、その暗号を解きやすくするためのCipher Disk（暗号円盤）です。現代の暗号は複雑な演算を伴うために、人力での解読はほぼ不可能です。

暗号化ってなに？

平文での通信は読めてしまう

暗号化していないと、攻撃者はどこでも盗んで読み放題

暗号化の魔法は内容を読めなくする



※1：暗号化方式　※2：「暗号キー」

暗号化したものを送れば攻撃者が読めない

※ただし、攻撃者が「シーザー暗号」を読めない場合

事前に決めておいた方法（暗号化方法）と呪文（「暗号キー」）で暗号文を復元（復号）する

暗号が破られる場合

暗号化方法の種類はいろいろ

シーザー暗号化方法
×　古い、危険すぎ

「WEP」方法
×　解読されるからだめ

「WPA」方法
○　呪文が長ければ安全

暗号破られる例①　呪文がバレている

暗号破られる例②　方法が古くて解読可能！

暗号破られる例③　呪文が簡単すぎて解読される

※このページは、抜き出して個別に使用することを想定して、本文と一部内容が重複しています。ご了承ください。

コラム：パスワードの管理と流出チェックについて

ここでは、パスワードの管理に関する最新の動向を踏まえて、本文でも紹介したテクニックを詳しく解説しましょう。攻撃者から身を守るためには、最新の技術で先手を打つのも一つの対策だからです。

パスワードに関して、2018年には約16億件のパスワードが流出したというニュースが流れました。また、有名ホテルチェーンが顧客情報約5億件を流出させたニュースも報じられました。こうして流出したIDとパスワードは、必ずといっていいほど不正アクセスに使われます。そういった攻撃から身を守るには手段は2つ。1つは、流出しても被害を最小限にとどめるため、サービス毎に別々の長くて複雑なパスワードを設定すること。もう一つはそもそもパスワードを盗めないようにすることです。

● パスワード管理アプリの高度な利用

パスワードに関して、NISCでは、「人は必ずヒューマンエラーを起こす」ことを前提に対処方法を考えます。例えば、パスワードの管理は数が多くなるほど覚えにくく、使い回しをせずサービス毎に別々のものを考えるのは面倒で、対策せずに強要すると、そのうちワンパターン化したり、同じ物の使い回しが起きたりするのではないかと考えます。

これを解決するため、総合的にパスワードを管理する、スマホの「パスワード管理アプリ」などを推奨します。パスワード管理アプリは、単にパスワードを保管してくれるだけではなく、条件を設定するとそれに合わせた長くて複雑なパスワードを自動的に生成してくれるほか、最近では、ウェブブラウザでのサービスログイン時に、自動的に起動してIDとパスワードを入力したり、アプリ起動時にもIDとパスワードを入力してくれたりするように進化しているものもあります。パスワードを、いちいち管理アプリを見て入力したり、カット＆ペーストしたりする手間も省きつつ、みなさんの負担を軽減する傾向にあるのです。

また、パスワード管理アプリの中には、多要素認証で利用する使い捨てパスワードを発生するためのQRコードを、アプリ内に読み込めるようになっているものもあります。多要素認証で使い捨てパスワードを利用する設定にすると、サービスそれぞれが別々の「ソフトウェアトークンアプリ」をインストールさせるように見えて、実は必要なのはこのQRコードを読み込ませることだけなので、パスワード管理アプリに読み込んで、一括して管理するようにできるのです。

加えて、パスワード管理アプリによってはスマートウォッチとの連携を行っているものもあります。これらのアプリでは、スマートウォッチにインストールされた連携用のパスワード管理アプリ上で、登録しているIDとパスワード、多要素認証用の使い捨てパスワードを発生させることもできるので、パソコンでウェブサービスへのログインに際して、スマホを立ち上げなくても、手元でログインに必要な情報をすべて確認できます。

これらを使って、楽に個別のパスワードを管理しましょう。どういったアプリが条件を満たすのか評価記事などを参考に検索して、利用するときは責任関係がしっかりとする有料のものを選択しましょう。無料のアプリには情報を抜き取ることを目的とするものも紛れ込んでいるからです。

● パスワードを無くすFIDO

主としてパスワードが流出するのは、サービス側で保管しているIDとパスワードを含めた個人情報が、多量にまとめて盗まれるケースです。したがって、サービス側に盗むべきパスワードがない場合は、この攻撃は成功しません。そのためにパスワードそのもの無くすことを目指すのがFIDOアライアンス（Googleやマイクロソフト、NTTドコモといったIT企業や通信会社、信販会社、通販会社などが加盟）が進めるFIDOという方法です。この方法では、利用者が「本人」

であるという認証をパソコンやスマホなどそれぞれの機器の上で行い、利用するサービスへは「本人だと認証しました」という情報のみをやりとりするのです。本人だと認証する方法は、USBセキュリティキー、指紋や顔認証などの生体認証です。

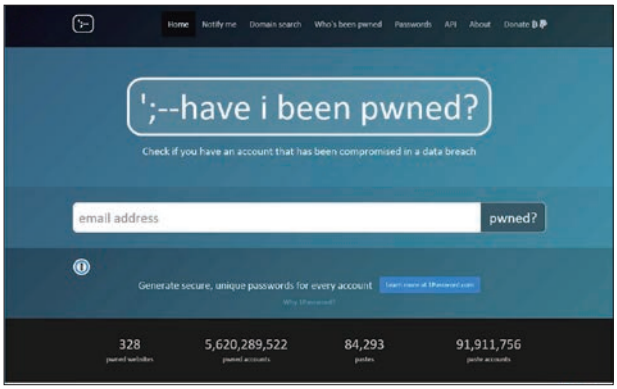
現在Googleのサービスの一部で利用が始まっているほか、最近はAndroidスマホ本体のFIDO2対応や、WindowsへのログインWindows Helloに対応した端末などがFIDO2に対応しています。

今後これらの方式が普及してきた場合、積極的に選択することも検討しましょう。少なくともGoogleの社内では、FIDO2対応USBセキュリティキーを採用することで、フィッシング詐欺の被害がゼロになったと報告されています。

パスワード管理と認証の新しいトレンド

ハードウェアメーカーが推奨し、密接に連携するパスワード管理アプリと対応スマートウォッチや、FIDO対応機器。これらの導入がセキュリティの向上に役立ちます。

流出IDとパスワードチェックサイト「Have I Been Pwned?」（私、漏洩してる？）



メールアドレス流出チェックURL：https://haveibeenpwned.com/
パスワード流出チェックURL：https://haveibeenpwned.com/Passwords/

ほかにもFirefox Monitorなどで、同等の機能が提供されています。実績もありセキュリティ業界において評価は高いですが、あくまでも民間のサービスなので、その点を理解して利用しましょう。

● パスワード流出を能動的に検知する

パスワードの流出は、登録しているサービス側から流出の事実が通知されるほかにも、流出情報の検索サイトを利用すれば能動的に調べられます。

セキュリティ識者のトロイ・ハントさんが、流出したIDとパスワード情報を収集し検索できるようにした「Have I Been Pwned?」は、各国政府によって政府系メールアドレスの流出チェックなどにも使われていますし、個人でもウェブサイトで自分のIDとパスワードが過去に流出していないかチェックできるほか、アドレスを事前に登録しておくと流出時に警告のメールが送られてきます。

また、パスワードを入力して、そのパスワードが「流出した履歴あり」と出た場合、それは、あなたの情報の流出であってもほかの人の情報の流出であっても、以降パスワードリスト攻撃の対象になるので変更しておきましょう。

根っこは同じデータベースを用いますが、ウェブブラウザを提供しているFirefoxもFirefox Monitorとして同様のサービスを提供しているほか、パスワード管理アプリでもパスワードの安全性チェックに採用する動きが見られます。今後こういった流出情報のチェックサービスは増えていくと予測されるので積極的に活用して、攻撃される前に対処するようにしましょう。

2 通信を守る、無線LANを安全に利用する

私たちが、日常的にインターネットで送信するIDやパスワード、送受信するメールの文面やウェブサイトで閲覧する内容は、常に攻撃者の盗聴や盗み見の危険にさらされています。

攻撃者は、そうした情報を不正に入手して売却したり、様々な手段を駆使して直接お金を手に入れるために利用したりします。これを阻止するためには、通信している情報の暗号化が必要なのです。

そもそも、インターネットはその始まりにおいては、暗号化など全くされておらず、情報をそのままの状態(平文)で送受信するシステムでした。

インターネットは、蜘蛛の巣状に接続し合ったサーバ間で、どこかの経路が遮断されても迂回して通信を続ける、そういう面では先進的ではあったのですが、攻撃者などの悪意の存在を前提に構築されてはいなかったからです。

その後、インターネットの発展にしたがって、悪意を持ったものが現れ、コンピュータウイルスの開発や、パスワードを破って侵入しての情報の奪取、通信中の情報の盗聴が行われるようになり、それぞれ対策が必要になりました。

コンピュータウイルスにはウイルス対策ソフトが、パスワード破りには複雑なパスワードや二要素以上の多要素認証などが、そして、通信中の情報の盗聴には暗号化が、攻撃者への防御として普及していくわけです。

1 それぞれの状況に合わせた暗号化の必要性

一口に通信の暗号化といっても、様々な状況に合わせた、それぞれの暗号化があります。

私たちが通信すること一つをとっても、有線LAN、LTEなどの携帯電話回線、Wi-Fiなどの無線LAN、多様な通信手段があります。

このうち、攻撃者にとって、手軽に行いやすい攻撃の一つとして無線LAN通信の盗聴があります。

無線LANでは、その名のとおり通信機器が無線(電波)を使って通信するので、盗聴に際してなにか工作する必要はありません。通信が暗号化されていなければ、無線LANに対応したパソコンを持って電波が届く範囲にいるだけで、簡単に盗聴することが可能です。

なお、有線通信も暗号化されていなければ、通信経路上のどこかで情報を盗聴することが可能です。

さらに、攻撃者が利用者のふりをしてメールサーバやパソコンに侵入すれば、中にたまったメールや、内蔵記憶装置などの中の情報も盗み見し放題です。

パソコンがマルウェアに感染して、記憶装置の中の暗号化されていないファイルが流出し、見放題になるという事件もありました。

そういった状況を避けるためには、仮に盗聴されたり、侵入されたり、流出してしまっても、通信内容や重要なファイルの中身が見られないように、それぞれのシーンに応じた適切な暗号化をする必要があります。

その対策をあげていくと数え切れないのですが、このセクションでは、まず私たちの生活でもっとも身近な無線LAN通信の暗号化について説明しましょう。

2 無線LAN通信(Wi-Fi)の構成要素

インターネットに接続した無線LANアクセスポイントさえあれば、いちいちLANケーブルをつながなくても、気軽にインターネットを楽しめる無線LAN通信(Wi-Fi)。

家庭で利用する無線LANでも、外出時に利用する公衆無線LANでも、セキュリティがしっかりしていなければ、通信中に送信したIDやパスワード、データすべてを攻撃者に盗まれる危険性があります。

それを理解するために、まずは無線LAN通信を構成する要素を理解しましょう。

最初は、無線LAN通信を提供する「無線LANアクセスポイント」になる機器。一般には「無線LANアクセスルータ」「Wi-Fiルータ」あるいはシンプルに「ルータ」などと呼ばれます。この機器で無線LAN通信を提供する際、最低限以下の3つを設定します。

① 識別名「SSID(Service Set Identifier)」
②通信内容を暗号化するための「暗号化方式」

③その暗号化のための鍵となる「暗号キー」(設定上は暗号化キーと書かれる)

「暗号キー」は、利用者が無線LANアクセスポイントに接続するときパスワードのように使われるほか、通信内容を暗号化するときと、元に戻す復号(元の平文に戻す)のときの鍵として使われます。

ここまでが、無線LANアクセスポイントの構成要素です。

スマホやパソコンが無線LANを利用して通信するときは、利用する機器の無線LAN(Wi-Fi)設定で、SSIDを手掛かりに目的の無線LANアクセスポイントを見つけ、必要な場合は暗号化方式を選択し、「暗号キー」を入力して接続します。

なお、災害時や公益目的で、誰でも無線LANを利用できるように、「00000JAPAN(ファイブゼロジャパン)」を筆頭に「暗号化無し」で提供されている無線LANアクセスポイントもあります。この場合は利用時に暗号化方式も「暗号キー」も必要ありません。

次に、無線LANの危険要素について説明します。危険なポイントは以下の2つになります。

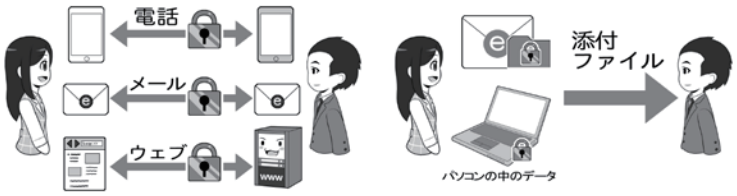
①「通信が暗号化されていないか、されていても安全ではない場合」
②「暗号化の鍵(「暗号キー」)が公開か漏れている場合」

3 暗号化無しや、方式が安全ではないものは危険

無線LANの利用において、通信が暗号化されていないものは、内容が平文で送受信されているので、別の手段での暗号化を行わないま

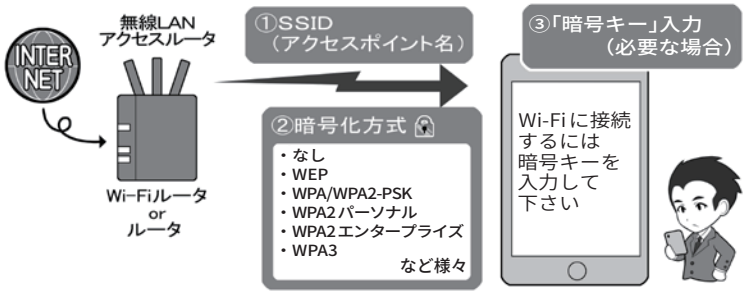
それぞれの状況に合わせた暗号化

通信の暗号化 **ファイルの暗号化**



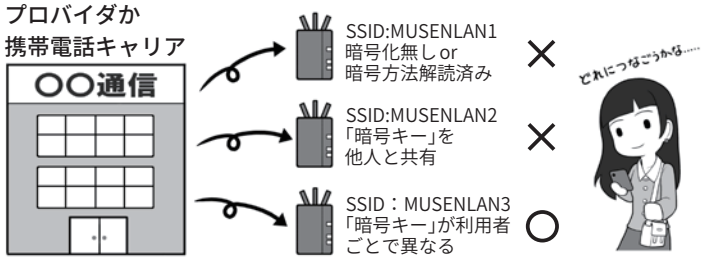
暗号化には、電話、メール、ウェブ閲覧などの「通信の暗号化」と、ファイルやパソコンの記憶装置などの「ファイルの暗号化」があります。

暗号を使う無線LANの構成要素



暗号化を伴う無線LAN通信には暗号化方式と「暗号キー」の設定が必要となります。「暗号キー」は機器に接続するときにパスワードのように使われます。

公衆無線LANが安全とは限らない



信頼がおける企業や団体でも、提供しているWi-Fiが安全とは限りません。アクセスの利便性のため暗号化無しで提供される場合もあるからです。

「暗号キー」共有は接続しちゃダメ

暗号化方式が安全でも、「暗号キー」を見知らぬ他人と共用するものは、すべて危険です。こういった方式は、公衆無線LANやホテル、公共機関、インターネットカフェやレストランなどで広く使われています。

提供する側が善意で行っていても、攻撃者は善意で行動しません。攻撃できる環境があると判断するだけです。

安全な通信のため、自前で暗号化を行うテクニックがなければ利用不可です。

ま使っていると、攻撃者に内容を盗聴されてしまいます。

そのため、まず「暗号化無し」のアクセスポイントは基本的には利用しないようにしましょう。

災害時など、例外的に使用する場合は、後述の「10 公衆無線 LAN が安全でない場合の利用方法」を参照してください。安全な利用には最低限、別の手段での暗号化が必要だと覚えておいてください。

暗号化無しの通信は、拡声器で遠くの人と話しているようなもので、耳を傾ければその場にいる誰もが内容を知ることができます。

また無線 LAN 通信が暗号化されていても、その暗号化方式がすでに破られていて安全ではない場合、上記と同様に、攻撃者は通信を盗聴して内容を解読することができるので、これも危険です。使用しないようにしましょう。

これは、「英語でしゃべればわからないだろう」と思ったら、周りにいた人も英語が理解できて、内容がばれるイメージです。

危険である暗号化方式の具体例としては、「WEP」という名前のものや、方式の名称の中に「TKIP」と含まれるものが該当します。

一方、暗号化方式として安全とされるのは WPA-PSK(AES)、WPA2-PSK(AES)、WPA2-EAP、WPA2- エンタープライズ、IEEE 802.1x、SIM 認証、そして、無線 LAN の多くの問題点を解決するために作られた WPA3、それらの記述があるものです。安全な方式の詳細は P69 を参照してください。

4 暗号化方式が安全でも「暗号キー」が漏れれば危険

暗号化の方式自体が安全でも、通信を暗号化するための「暗号キー」が漏れていると、通信を盗聴した攻撃者が通信内容を復号したり、同じ SSID と「暗号キー」を使って偽の無線 LAN アクセスポイントを作り、本物のアクセスポイントになりすまして通信内容を根こそぎ奪う、中間者(Man-in-the-middle)攻撃を行ったりすることができるようになります。

イメージとしては、破られていない暗号化方式は誰も知らない言語で、「暗号キー」が辞書。しかし、辞書がほか人の手に渡っていると、たとえ知られていない言語でも解読されてしまうし、その情報をもとに通信する相手になりすますこともできる、というものです。

この至極単純な、「暗号キーが漏れていれば暗号化された通信を復号し解読できる」ということも、よく覚えておいてください。

5 家庭内での安全な無線 LAN の設定(暗号化方式)

家庭内で無線 LAN を使用する場合、先ほど説明した安全な暗号化方式である WPA-PSK(AES)、WPA2-PSK(AES)、WPA3 を利用し、「暗号キー」を P54 の基準にしたがって、完全にランダムで充分に長くして、さらに、その「暗号キー」を「家族だけが知っている」状態に保てれば、ほぼ安全に使用することができます。

これを実現するため、無線 LAN 機器設置時には、まず機器を購入したときの初期の「暗号キー」は変更しましょう。上記のとおり、家族だけしか知らない「暗号キー」に変更しなければなりません。メーカーによっては「暗号キー」が共通だったり、付け方に規則性があるかもしれないからです。

また、極端な考え方をすれば、その機種がメーカーから手元につくまでに、初期の「暗号キー」を見たものがいないともいい切れません。

なお、SSID を変更する場合、自分や家族の名前、家族を想起させる語句は使わないようにしましょう。あなたが攻撃のターゲットの場合、攻撃するべき無線 LAN を特定させるヒントになるからです。

家庭用無線 LAN アクセスルータは、標準で 2 つ以上の SSID を持てるものが多く、そのうちの一つには、WEP などのもはや安全でない古い暗号化方式が設定されている場合があります。これは、主に古いゲーム機などが接続できるようにするためだったりします。

しかし、こういった設定はセキュリティ上の穴となるので、設定を変更し、安全な暗号化方式にするか、安全でない暗号化方式の設定のものはすっぱりと停止しましょう。また、接続する古い機器が安全でない暗号化方式しか選べないならば、使用は諦めましょう。

同様に、来客用に簡便な「暗号キー」や、問題のある暗号化方式を使った接続設定があれば、これも停止しましょう。来客に家族用の SSID に接続させるのも安全ではありません。「暗号キー」が「家族だけが知っている状態」ではなくなってしまうからです。

どうしても来客用に一時的にアクセスポイントを開放したい場合は、2 つの SSID の一つを来客専用にし、2 つのアクセスポイントの間で、お互いのアクセスポイント

に接続した機器が見えないような分離状態に設定してから提供しましょう。そして、来客が帰宅したら、そのSSIDは利用停止しましょう。

6 家庭内での安全な無線LANの設定（そのほか）

無線LANアクセスルータには、ウェブブラウザを使って本体の設定画面にアクセスするための、機器管理用のIDやパスワードがあります。それは、管理者アカウントとも呼ばれます。

こちらのパスワードも、必ず購入時のものから変更しましょう。このパスワードはログイン画面から使用するものなので、「ログインパスワード」の基準に従い変更しましょう。

この設定画面が、もし家の中からだけでなくインターネット側からアクセスできるようになっていたら、アクセスできないように変更しましょう。また、設定画面が無線LANで接続した機器からアクセスできず、有線LANからのみアクセスできる設定にしましょう。この設定をする理由は、家の外にいる攻撃者が姿を隠した上で無線LANに接続し、設定内容を変更したりしてしまわないようにするための予防策です。

無線LANアクセスルータにルータ本体と機器のボタンを押すだけで簡単に接続できる「WPS」「AOSS」「無線LANらくらくスタート」といった名称のもの、もしくは類似の機能がある場合は利用不可にしましょう。この設定をONにしていると、目を離したすきに、利用してほしくない人物が、ボタ

家庭でのWi-Fiの利用

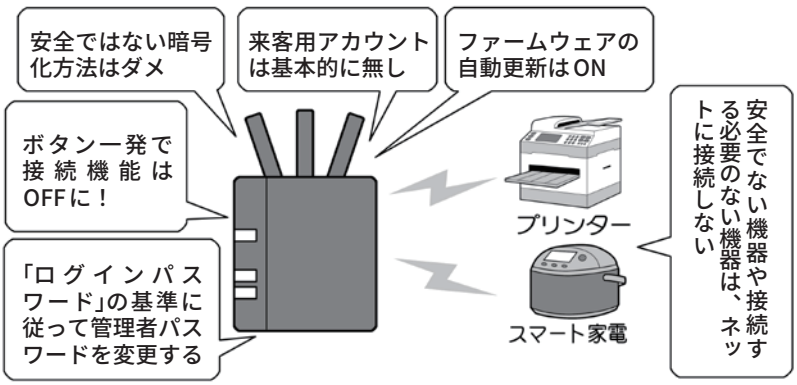
①出荷時の管理者パスワード、「暗号キー」の変更

出荷された機器は、厳密にいえば誰かの手によって梱包されているので、出荷時の「暗号キー」が見られている可能性があります。必ず変更しましょう。

②「暗号キー」は家族のヒミツ

家庭で使える暗号化方式は、「暗号キー」を家族のみの秘密にすることが、安全に使うための絶対条件です。ほかの人には教えないようにしましょう。

③ルータと機器の安全な運用



家庭で無線LANや有線LANを使用する場合、注意したり設定を変えたりしなければならない点がたくさんあります。必ずチェックして安全な状態を作りましょう。また、基本的に接続する必要がない機器を、むやみに家庭のLANに接続しないようにしましょう。

ン一発で手元の機器を無線LANに接続できてしまうからです。

どうしても利用する場合は、設定画面からそのときだけONにして使用し、設定後はOFFにします。

UPnP（Universal Plug and Play）の設定も、不用意に家庭内のLANの機器をインターネット上に公開してしまう可能性があるので、OFFにします。そして、ネットに接続する必要のない機器は、無線・有線にかかわらず、そもそもLANに接続しないようにしましょう。

無線LANアクセスルータの設定画面に、本体ファームウェアの自動アップデート機能がある場合はONにしておきましょう。それによりメーカーがルータの不具合（バグ）などを修正した場合、自動で更新が行われセキュリティが最新の状態に保たれます。

もし自動アップデートの設定がない場合は、自分のスマホに定期的な通知を作り、それにしたがってファームウェアが更新されていないかチェックし、公開されていれば更新処理を行いましょう。

なお、昔に書かれたセキュリティの解説記事によっては、「SSIDを隠すステルス設定」や、接続できる機器をLAN機器の番号で制限する「MACアドレス規制」を対策として推奨していたりします。

しかし、ステルスになったSSIDも簡単に探し出すことが可能ですし、MACアドレスは盗聴可能かつ詐称可能ですので、これらの対策を行っても安全性は向上せず、むしろ利便性が悪くなるので、設定する意味はないでしょう。

無線LANアクセスルータは、家庭のセキュリティの要です。お使いのルータに上記のようなセキュリティの設定がない場合や、安全な暗号化方式の設定がない古い機器の場合は、速やかに利用を停止し最新のものに買い換えるようにしましょう。

7 公衆無線LAN利用時の注意

公衆無線LANの安全な利用は、家庭用の無線LANの安全な利用と少し事情が異なります。

例えば、公衆無線LANで「WPA-PSK（AES）/WPA2-PSK（AES）」の方式の無線LANが提供されていた場合、暗号化方式自体は安全でも、別の危険があります。

上記の名称の中のPSKの部分はPre-Shared Keyの略です。利用にあたり「暗号キー」を事前に共有する方式のことで、この方式では家庭内の利用のときと同様に、複数の人で同じ「暗号キー」を使うことになります。これを公衆無線LANに当てはめると、全く知らない人と、同じ「暗号キー」を一緒に使うことになるわけです。

その設定を使って通信を行うと、「暗号キー」を知っている攻撃者により、通信内容を直接盗聴されたり、なりすまし無線LANアクセスポイント（偽アクセスポイント）をしかけられ、通信内容が盗聴される可能性を避けられません。

しかし、この方式を含め安全でない暗号化方式は、街中のカフェやレストラン、ホテル、あるいはインターネットプロバイダや携帯電話キャリが提供する公衆無線LANでも広く使用されています。これらのアクセスポイントはすべて危険ということになります。

こういった危険なアクセスポイントを使用する場合、無線LAN通信の暗号化とは別の暗号化機能で対処する方法もがあります。それについては後述します。一方、安全な暗号化方式の選択で安全性を確保する方法もあります。

8 個別の「暗号キー」を用いる方式の公衆無線LAN

公衆無線LANにおいて通信の安全を確保する方法は、危険な暗号化方式などを使わないことは当然として、「暗号キー」を他人と「共有しない」で個別の「暗号キー」を用いる方式を利用することです。

この方法は、公表されている公衆無線LANアクセスポイントの情報の中で「WPA2-EAP、WPA2-エンタープライズ、IEEE 802.1x、SIM認証」といった用語が含まれるものを選択するのです。

携帯電話キャリアなどは、いくつかの異なる暗号化方式の公衆無線LANを提供している場合があり、ウェブサイトなどで、それぞれのSSIDが採用している暗号化方式が、きちんと掲示されている場合があります。

利用前にそこをチェックし、上記の方式名を頼りに、安全な接続ができる公衆無線LANのSSIDを探してから利用しましょう。

「WPA2-EAP、WPA2-エンタープライズ、IEEE 802.1x、SIM認証」などが公衆無線LANとして安全である理由は、これらの方式の無線LANアクセスポイントを利用する場合、公衆無線LANサービスの提供者が、利用する一人ひとりの機器、または、利用者を識別して個別の認証を行い、個別の「暗号キー」を用いて通信を行うからです。

そのため、他人と同じSSIDに接続しても、自分の「暗号キー」を他人に知られることがないのです。

一例を挙げると、「SIM認証」と呼ばれる方式では、それぞれのスマホなどに入っているSIMカードの情報を用いて認証＝接続許可を出すわけです。SIMは1枚1枚別々の情報が入っているので、誰かと「暗号キー」が被ることなく安全な通信が確保されるわけです。

9 公衆無線LANに関して新規に購入したスマホなどで行うこと

新規契約や機種変更、携帯電話会社の乗り換えなどをして、携帯電話キャリアで新しいスマホを手に入れたら、まずやるべきことがあります。

そのスマホには、携帯電話キャリアで提供している様々な方式の公衆無線LAN用の自動接続設定が、安全性に関係なくまとめて導入されていることがあるからです。

購入後、細かい設定をしなくても自動的に公衆無線LANに接続できるので便利と思われがちですが、この状態では、意図せず「安全でない方式の公衆無線LAN」に、接続してしまう可能性があります。

新しいスマホなどを手に入れたら、まず接続される可能性があるアクセスポイントの暗号化方式を調べましょう。安全でない公衆無線LANのアクセスポイントに接続してしまった場合、無線LAN接続を切断して、その接続用のプロファイルも削除し、できれば二度とそのアクセスポイントに自動接続されないようにしましょう。

また、知らない公衆無線LANア

公衆無線LAN通信の表示の意味

①スマホやパソコンの画面から見た無線LAN暗号化

接続	Android	iOS、mac OS	Windows
×（暗号化無し）			
△（暗号化有り）			 ＊1

②詳細な区分けから見た無線LAN暗号化

接続	ネットワークの種類	暗号化キー（「暗号キー」）		解説
×	暗号化無し		なし	暗号化無しは論外
×	WEP		事前入手	解読済み。使用は不適切
×	WPA-PSK WPAパーソナル	（TKIP）	事前入手	TKIPには暗号化にセキュリティ上の不安あり。AESは暗号解読不可能とされているが、「暗号キー」が事前に存在し、利用者はみな同じものを共有するので、暗号解読の可能性あり
△		（AES）	事前入手	
×	WPA2-PSK WPA2パーソナル	（TKIP）	事前入手	
△		（AES）	事前入手	
○	WPA2-EAP＊2 WPA2エンタープライズ	（AES）	SIM認証（端末個別）＊2 個別パスワード、クライアント証明書認証（利用者個別）	SIM認証ではSIMの情報を認証に用い、個別の「暗号キー」が利用されるので通信内容の不正な解読は困難。ほかにも利用者を個別に認証するEAP-TTLS,EAP-TLSなどの方式もある

上の表は、Android、iOS、mac OS X、Windowsなどで、無線LANアクセスポイントを選択するときの画面に表示されるアイコンの例になります。それぞれ2種類のアイコンしかありません。そして、このアイコンは、各アクセスポイントが信頼できるかを表しているのではなく、単純に「暗号化されているかどうか」だけを表しています。

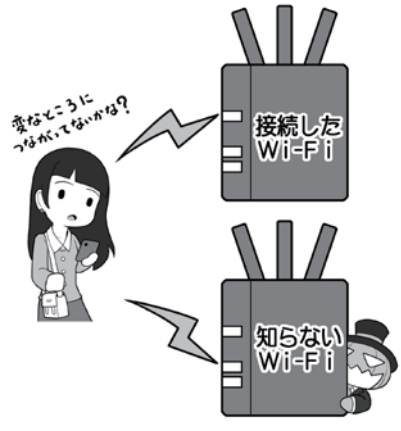
下の表は、暗号化方式のそれぞれの安全性とその理由を書き出したものです。この2つの表を比較すると、すでに暗号化が破られており、利用が推奨されていない「WEP」が、表示アイコン上は暗号化に分類されていることがわかります。アイコンは暗号化の有無を表しているので、これは正しい表示ですが、アイコンは安全性の担保ではないと認識して下さい。Androidは、接続したアクセスポイントをタップすると「セキュリティ」の項目でネットワークの種類の暗号化方式などを確認できます。Windows、mac OS Xは調べるのに手間がかかります。iOSでは、簡単に確認する手段がありません。

なお、WPA3が普及すると、これらの問題点のかなりが解消されるようになります。

＊1：Windowsでは、バージョンによってアイコンに「セキュリティ保護あり」と表示される場合もあります。

＊2：例としてはNTTドコモでアクセスポイントの名称（SSID）が「0001docomo」、auで「au_Wi-Fi2」、ソフトバンクで「0002softbank」のものがWPA2-EAPの方式です。各携帯電話キャリア提供の無線LANアクセスポイントの一部で、自動接続になっているため意識することはありません。そのほかの安全性が確保されていないと判断したアクセスポイントに接続されている場合は、接続を切ることが推奨されます。

新しいスマホを購入したら…



携帯電話キャリアなどで購入したスマホには、無料提供されている公衆無線LANの設定が入っています。しかし、すべての公衆無線LANが安全とは限りません。それぞれの暗号化方式を調べ、安全でないものに接続したら切断するようにしましょう。

また、知らないアクセスポイントに接続した場合も切断しましょう。攻撃者が設置したものだったり潜んでいたりすることがあります。

クセスポイントなどに勝手に接続されてしまった場合は、同様に設定を削除して、以降自動で接続されないようにしましょう。

10 公衆無線LANが安全ではない場合の利用方法

しかし、いつでも安全な状態の公衆無線LANを利用できるとは限りません。先ほど少しだけお話しした観光客用や、災害時に設置される「00000JAPAN」などの「暗号化無し」の公衆無線LANしか利用できない状況も考えられます。

しかし、「暗号化無し」もしくは「危険な状態」で提供されている無線LANアクセスポイントを不用意に利用すると、攻撃者から見れば獲物が絶好の狩り場に飛び込んできた状況になってしまいます。

対策は、「無線LANの暗号化に頼らず、自前で通信を暗号化して盗聴対策をする」ことです。

もし、この言葉の意味が理解できない場合は、ここからはややハードルが上がりますので、無理をせず自前の携帯電話回線、もしくはパソコンならばスマホをルータ代わりに利用する「テザリング」の範囲で、手軽かつ安全にインターネット接続することをおすすめします。

11 自前の暗号化による盗聴対策

自前の暗号化で盗聴対策をする第一歩は、ウェブブラウザでのインターネット閲覧では「https://」から始まるもののみ、メールでは「SSL/TLS」を使った通信設定になっているもののみ、スマホなどのアプリでは暗号化通信でサーバに接続するもののみ使うことです。

前者2つに関しては、後ほどそれぞれ詳しく説明します。

スマホアプリに関しては、アプリの通信全体を暗号化するトレンドに向かいつつありますが、現状、提供している会社によっては通信を暗号化しているかどうか明確にしていないものも多く、技術者でもない限りは自分で確認することは困難です。

アプリが通信を暗号化しているかどうかは、調査結果など公開されている情報から確認するか、多くの人が使用していてかつ盗聴や情報流出のトラブルがないもの、という選択しかありません。

もしくは、通信の全暗号化を商品として表明しているアプリに限定して利用することです。

12 まとめて暗号化するVPN、現状は過信できないが今後に期待

こういった個別の面倒な対策ではなく、まとめて一気に対策をする方法もあります。それは、VPN（Virtual Private Network：仮想プライベートネットワーク）の個人利用です。

VPNとは、元々は一つの会社の離れた事業所間をインターネットを使いながら接続する技術です。まるで会社内のLANで接続されているように、秘密を守りつつ互いに通信することができます。VPNはインターネットを使って事業所間を接続してますが、その通信が外部から盗聴できないように暗号化して秘密を守っているのです。

この方式を「事業所から事業所」ではなく、「個人の機器から安全な場所にある出口サーバ」に置き換えて利用するのが、VPNの個人利用です。

この場合、通信は自分のスマホやパソコンから、少なくとも安全な場所にあるとされる出口サーバまで、無条件ですべて暗号化されるので、どのようなソフトやアプリでも、また、その間の公衆無線LANの暗号化方式が安全でなかったり、そもそも全く暗号化されていなかったりしても、攻撃者に盗聴される心配は少なくなります。

ただ、このVPNの使い方はまだ、一般の利用者が豊富な選択肢の中から選び、ボタン一つで簡単に使える程にはこなれていません。現状は、一部プロバイダが有料サービスで提供していたり、あるいは有料アプリで提供されていたりする程度で、無料で安全性が高く手軽に使えるものは、自分で設定画面を書き換える必要があるなど、導入にスキルが求められます。

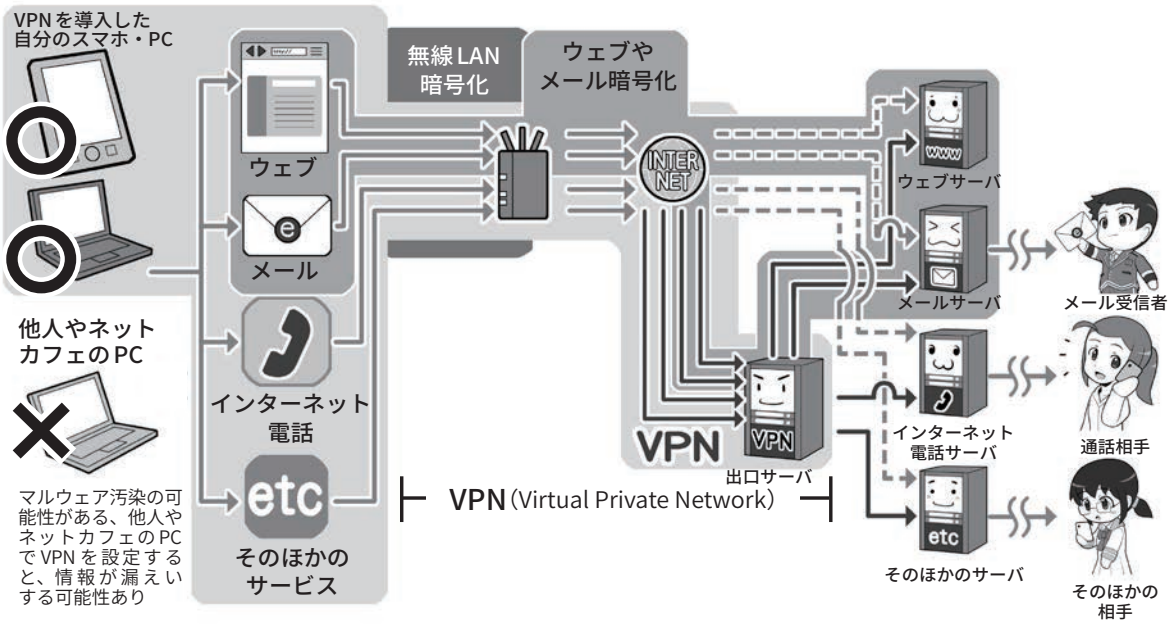
また、利用するVPNのサービスによっては、誤ったアクセスポイントに誘導されたり、VPN接続が切れると暗号化されていない状態に移行して通信を継続したりしてしまうものもあるなど、2020年の春の時点でも、まだ決定版的なサービスがありません。

どうしてもVPNを利用したい場合は、そういった問題点に関する各VPNサービスのテスト結果を公開しているウェブサイトがあるので、そこできちんと問題点に対応しているVPNサービスを探し、導入するようにしましょう。

なお、VPNが通信を暗号化するのは出口サーバまでなので、その先の通信の暗号化が行われない点は注意しましょう。

様々な場所から安全なアクセスを可能にするVPN

①詳細なVPNのイメージ

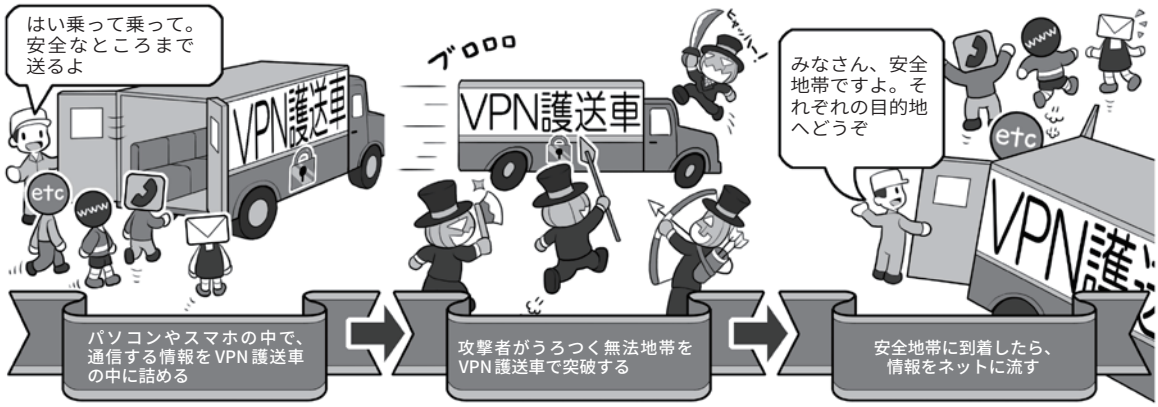


VPN を図で説明すると、上のように入り組んでよく分からなくなってしまうので、簡単な図を下に用意しました。くじけそうな方は、まず下をご覧ください。

上の図では、左から右に向かって通信を行う場合、無線 LAN の暗号化、ウェブやメールの暗号化、VPN とそれぞれ暗号化の守備範囲があることが分かります。

無線 LAN の暗号化は範囲が短く、ウェブやメールの暗号化は文字どおり用途が限定されます。VPN はすべての通信を暗号化し、かつ広範囲にカバーしてくれます。しかし、その範囲は利用者の機器から安全と思われる場所に設定された出口サーバまで限定なので、その先の目的のサーバまでは暗号化されない区間が残ります。VPN さえあればすべて安全というわけではないのです。

②簡単なVPNのイメージ



VPN を簡単なイメージで説明すると、この図のようになります。スタート地点（自分のパソコンやスマホの中）でデータを護送車に乗せて全部まとめて暗号化、危険地帯を突破し、信頼がおける安全な場所（出口サーバ）に着いたらデータを解放します。VPN は暗号化されていない無線 LAN を利用するのにも役に立ちますし、危険性があると思われる通信回線の盗聴、検閲や監視がある国からの安全な通信にも役立ちます。

また、災害時などに利便性を優先して提供される、暗号化無しの公衆無線 LAN を利用する場合でも役に立ちます。ただし、そもそもだれが運営しているのかよく分からないような無線 LAN アクセスポイントには、多分に攻撃者が潜んでいる可能性があるので、攻撃の手段は予測できず、VPN を使えたとしても積極的な利用は推奨しません。

3 ウェブサイトを安全に利用する、暗号化で守る

1 無線LANの暗号化とVPNの守備範囲

インターネット通信の基本は、「平文」での送受信です。ウェブサイトを見るときに、ウェブブラウザ上部のアドレスバーと呼ばれるウェブサイトの住所(URL)を入れる欄内が①http://で始まっている、②「保護されていない通信」や「安全ではありません」と表示されている、③先頭に注意喚起のⓘや🔏のマークがある場合、その通信は平文で送受信されています。

平文での通信は、通信の途中、攻撃者によっていつでも盗聴や改ざんされ、すべてもしくは一部が偽の情報に書き換えられる可能性があります。そうさせないためには、ウェブサーバとの通信の暗号化が必要になります。

前項では、通信の暗号化を行うために、無線LAN通信の暗号化と、VPNが登場しました。

利用者が目的のウェブサーバなどと通信するとき、無線LAN通信の暗号化では、利用者の機器から無線LANアクセスポイントまでの、すべての通信が暗号化されます。一方、無線LANアクセスポイントから、目的のウェブサーバまでの通信は、無線LAN通信ではないので暗号化されません。

一般の利用者向けのVPNサービス(以下VPN)では、利用者の機器からインターネット上の安全な場所にある出口サーバまで、無線であっても有線であってもすべての通信を暗号化します。しかし、出口サーバから目的のウェブサーバまでの通信は暗号化してくれません。

それぞれの守備範囲があり、攻撃できるポイントが残るわけです。

では、無線LANやVPNでは暗号化してくれない区間の通信の暗号化や、前項にあった、なんらかの理由で無線LAN通信の暗号化やVPNが使えない状況で安全に通信をしたい場合、どのような対処方法があるのでしょうか。

代表的なものとしては、ウェブサイト閲覧やメール送受信、通信の目的に限定して、利用者のそれぞれのソフトやアプリから目的のサーバまでを暗号化するやり方があります。

2 すべての通信と、その一部であるウェブサイトとの通信

無線LAN通信の暗号化とVPNでは、暗号化対象を「すべての通信」と書きましたが、ウェブサイトを閲覧するための通信の暗号化は、その「すべての通信」の中の一部「ウェブサイト閲覧に関する通信」に限定した暗号化になります。

通信には、ウェブサイト閲覧やメール送受信のほかに、インターネット電話、一部のアプリや特殊な機器など、目的などに応じて多様な通信が存在します。

例えるなら、すべての通信は「テレビの電波放送」という大きなくくり。これに対してウェブサイトを閲覧する通信は、その中の一つのチャンネルにあたります。そして、通信には様々なチャンネルが存在するわけです。

インターネットの通信では、このチャンネルにあたるものを「ポート」と呼び、ウェブサイトの閲覧の通信は、通常「ポート80」「80番ポート」という名称で、文字どおり80番のポートで行います。

80番ポートを使って送受信される通信は、基本的に暗号化されていない平文で、仮にこの状態でIDやパスワード、個人情報などを送信すると、通信を盗聴している攻撃者は特になんの工夫をしなくても情報を盗むことができます。また、情報が送受信ともに改ざんされ、偽の情報で取引などをさせられる可能性もあるのです。

それを避けるため、ウェブサイトを安全に閲覧する通信の暗号化が普及しました。それが「SSL(Secure Sockets Layer)/TLS(Transport Layer Security)」(以下SSL/TLS)という暗号化通信です。

暗号化していないウェブサイト閲覧では、URLが「http://」から始まるのに対して、SSL/TLSの通信では「https://」で始まります。後ろに追加されたsは「secure=安全な」の意味のsなのです。

3 httpsで始まる暗号化通信にはどんなものがあるか

先ほどのチャンネルの話に戻ると、httpsは通常ポート443を使

用します。つまりテレビのチャンネルを443にあわせたら、放送にはモザイクがかかっていて、有料放送契約者だけがモザイクを解除して見ることができる、というイメージです。

https://から始まるウェブサイトにアクセスすると、通信相手が誰であるかが後ほど説明する電子証明書によって証明され暗号化通信が始まり、アドレスバーに暗号化を示す鍵マークが表示され、問題がないという意味で、左ページの②や③の表示がなくなります。

この状態になると、「一応は」、IDやパスワードなどを入力しても大丈夫で、「表示される情報も改ざんされていない」ということになります。しかし、なぜ「一応は」かというと、最近ではこの状態でも安全とは限らないからです。

httpsによる暗号化通信を行うためには、まず、httpsで通信するサーバを作りたい企業や団体のサイト運営者が、認証局という機関に、書類で自分の会社の情報とサーバのドメイン名を提示して、ネット上で身元を明らかにする電子証明書の発行を申請します。

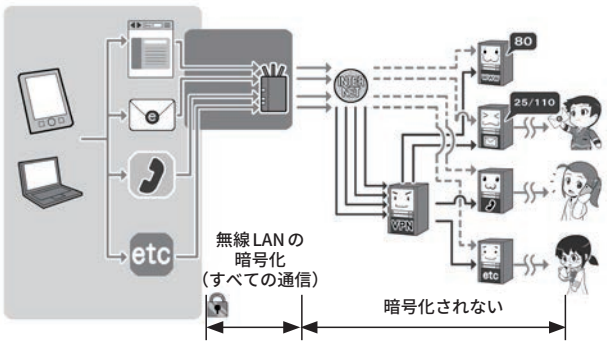
認証局は審査の上、その企業や団体が実在することを確認できれば、「SSL証明書(SSLサーバ証明書)」という電子証明書を発行します。

「SSL証明書」を取得した企業や団体は、httpsで通信するサーバに「SSL証明書」を設定し、利用者がアクセスしたときに、その「SSL証明書」によって、該当のドメインの運営主体と証明することで、互いに安心して暗号化通信が始められるようになります。

しかし、SSL証明書の中には実在性確認をせず、簡単なオンライ

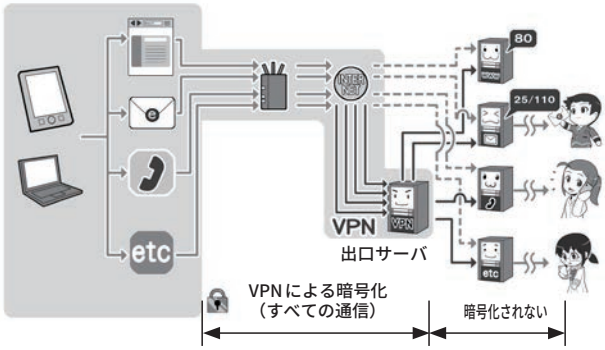
それぞれの暗号化の守備範囲

無線LANの暗号化



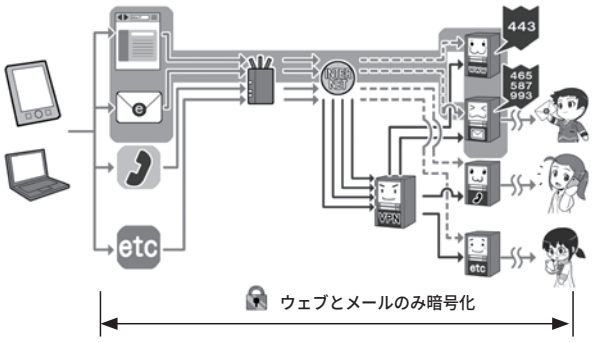
無線LANの暗号化は、利用者の機器から無線LANアクセスポイントまでのすべての通信を暗号化します。

VPNによる暗号化



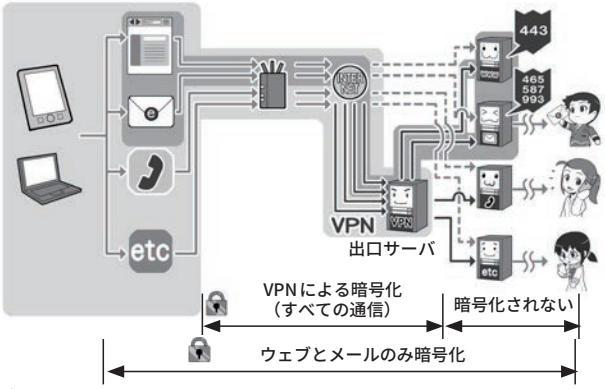
VPNは利用者の機器から、安全とされる「出口サーバ」までの区間で、すべての通信を暗号化します。

ウェブサイト、メールの暗号化



ウェブやメールの暗号化は、利用者のウェブブラウザやメールソフトから目的のサーバまでの区間で、ウェブとメールの通信だけを暗号化します。

VPN＋ウェブメールの暗号化



ウェブやメールの暗号化とVPNを組み合わせて利用することももちろん可能です。この場合暗号化される通信範囲は広くなります。

ンでの確認だけで機械的に発行し、企業や団体名すら証明書に記載しないものもあります。そのような「SSL証明書」は誰でも取得できてしまいます。

攻撃者は、そういった審査の甘い認証局を使って、詐欺サイトのための「SSL証明書」を取得して、暗号化通信をする詐欺サイトを立ち上げます。

そして利用者に、「あ、暗号化しているから大丈夫」と油断させ、パスワードやクレジットカード番号を入力させ盗むという事例が発生するようになったのです。

4 より厳格な審査の「EV-SSL証明書」

そういった問題に直面して、より審査を厳しくした「EV-SSL証明書」が登場しました。

「EV-SSL証明書」の審査では、証明書を発行する認証局も、外部の監査により基準を満たした者に限定して発行権限が与えられ、証明書を受ける側の企業なども、法的な存在の証明や、管理責任者や役員など複数人への聴取など、従来よりも厳格に審査が行われます。

これにより、「法的・物理的実在性」と「正当性」、結果としての「安全性」などが担保され、詐欺サイトなどの排除が行えるようになったわけです。

この「EV-SSL証明書」に対応したブラウザでは、アドレスバーが緑色になったり、企業名や団体名を表示したり、証明書に会社の所在地が表示されるなど、利用者がより確認しやすい表示が行われるようになりました。

しかし、現在はこういった表示を取りやめ、本項の最初に掲示したような表示に戻ったブラウザもあります。

その理由は、「EV-SSL証明書」特有の表示を行っても、利用者の行動に変化はなかったからとされ、平たく言えば、「利用者はそのようなものを確認しなかった」ということでした。

5 アドレスバー警告表示と、常時SSL化の流れ

また、そもそもウェブの通信が改ざんされないように「常時SSL化」「暗号化されている状態を標準とすべき」という流れもあり、「利用者が通信をきちんと暗号化しているウェブサイトの運営主体を確認しやすくする」方式から、「通信を暗号化していないウェブサイトを『危険である』と警告する」方法にブラウザを取り巻く動向が変化しました。

そして、本項の冒頭にあったように、暗号化されていないウェブサイトにアクセスしたときは、ブラウザが「安全ではない」と表示したり、警告表示のマークをつけたりするようになったのです。

なお、現在でもパソコンのブラウザなどでは、鍵マークをクリックすると証明書内容が表示されます。

「EV-SSL証明書」を利用しているサイトの場合は、その証明書の詳細まで表示すると、証明書を持っている企業や団体の所在地も表示されるので、そのサイトが自分が見ようとしているサイトかどうか判断する手掛かりになります。

スマホの場合は、鍵マークをクリックしても証明書が表示されない場合があるので、残念ながら普遍的に安全性を確認できる方法ではありません。

6 有効期限が切れた証明書は拒否する

なお、電子証明書には有効期限があり、失効したものは安全ではないと考えるべきです。

有効期限に問題があるなどの理由で、ウェブブラウザやセキュリティソフトが警告を発する場合、そのウェブサイトには接続しないようにしましょう。

きちんとセキュリティに対して必要な手続を行っている会社ならば、証明書の失効前に更新の処理を行い、新しい証明書に差し替えるはずです。

それを行わない企業は、セキュリティに対して必要な措置をしていないと判断し、したがってそのウェブサイトは安全に利用できないと考えるべきでしょう。

7 ほかにも証明書に関する警告が出るウェブサイトは接続しない

証明書が失効している警告以外にも、証明書に関する警告が表示される場合があります。

詳しく分類すると多岐にわたるので、すべては記述しませんが、以下のような例が該当します。

1. 証明書の使い方を間違っている場合
2. 証明書の署名アルゴリズムに問題がある場合
3. 証明書を発行した認証局になんらかの問題がある場合
4. 「オレオレ詐欺」のように認証

局でないのに認証局と偽って証明書を発行し、それを使っている場合（通称：オレオレ証明書）

いずれの場合も、「安全ではない通信」の元凶となります。

証明書の有効期限の問題と同様に、ウェブブラウザやセキュリティソフトが「証明書に関する警告」を発した場合、そのウェブサイトとの通信は安全でないと判断し、利用しないようにしましょう。

さて、ウェブサイトを安全に利用するには、通信面のほかにも気をつけるべきポイントがあります。

ほかのセクションとも重複しますが、ウェブを使うというくくりで少し触れておきましょう。

8 ウェブサービスのログインは多要素認証を選択する

ウェブサービスを安全に利用するには通信の暗号化も大切ですが、ウェブサービスにログインするIDやパスワードの管理と運用も大切です。

通信を暗号化しても、スマホやパソコンがマルウェアに感染してしまえば、通信する前の段階で情報が盗まれてしまいますし、ウェブサービスのIDやパスワードが盗まれると、攻撃者がウェブサービスに勝手にログインして、悪さをすることができるからです。

これを避けるため、P22でも触れたように、ウェブサービスへのログインは、使い捨てパスワード（ワンタイムパスワード）を含む、二要素以上の多要素認証を利用して、仮にパスワードが盗まれた場合でも攻撃者が簡単にログインできないようにしましょう。不審な

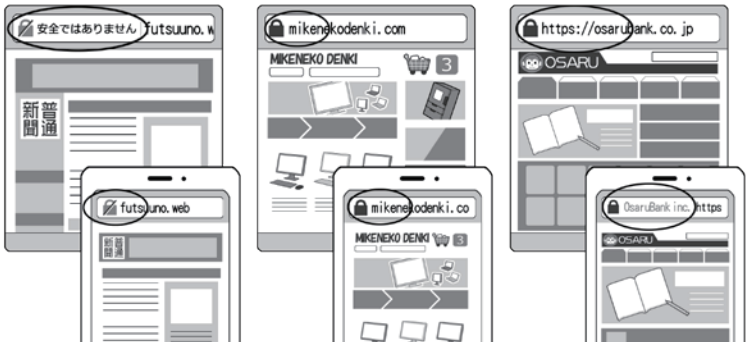
httpsの暗号化通信で情報を守る

個人情報の入力は基本的には……

ダメ ✕ 暗号化無し（httpと表示される）安全ではないと表示される ⓘや🔒マークがある

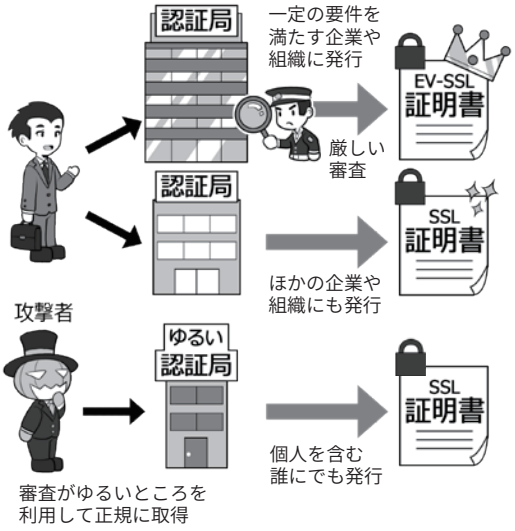
注意 △ SSL（暗号化あり）（httpsと表示される 🔒マークが表示される）

より安全 ○ EV-SSL（暗号化あり）（🔒マークと、一部のブラウザでは文字が緑になる）



個人情報の入力をする場合、暗号化は必須となります。厳しい認証局の審査を伴うEV-SSLのウェブサイトを利用する方が、より安全であると判断しましょう。特に、お金関連のサイトはEV-SSLの方がより推奨されます。

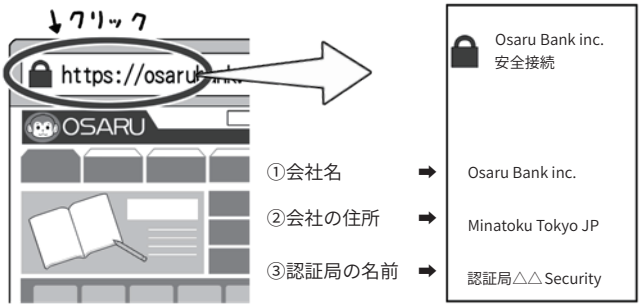
攻撃者が不正に取得した証明書に注意



SSL証明書には、ウェブサイトを運営する企業や組織が実在することを認証局が審査して証明してくれるものと、その機能がないものがあります。SSL証明書は元々、サーバ設置者の身元証明のためのものですが、最近では実在証明がなくても証明書を取得できる手があるので、攻撃者が攻撃サイト用に取得することもあります。

EV-SSLのhttpsサイトは、より厳密なので不正取得は困難ですが、上記のとおりただのhttpsサイトは運営者が不明な場合もあるので、要注意です。

証明書の内容をチェックする



パソコンなどの場合は簡単に証明書の内容をチェックすることができます。会社名や認証局の名前、EV-SSLに対応したウェブブラウザならば会社の大まかな住所も表示されます。また、一部ブラウザである緑文字のURL表示はEV-SSL証明書の証でもあるので覚えておきましょう。

ログインがあった時にログイン通知を受けとれる機能があれば利用して、攻撃を即座に察知できるようにしましょう。

また、近年、ウェブサービスへのログインに関して、そもそも「ネットを通じて認証のためにパスワードを送信する」という構造そのものが危険だという考え方も出てきています。正当な利用者である認証は、手元の機器の中で行い、パスワードなどは送信せず、「本人であることを確認できた」という認証情報だけをサーバに送って、ウェブサービスを利用可能にする、FIDOなどの方式も一部で採用が始まっています。

今後の動向に注目して、必要に応じて採用するようにしましょう。

9 多要素認証すら破る「中間者攻撃」

ウェブサービスの安全な利用のためには、二要素以上の多要素認証を利用するべきと第3章の1で書きましたが、それすらやぶる攻撃もあります。

例えば、パソコンから二要素認証に対応したインターネットバンキングを利用する際、銀行のサイトにIDとパスワードでログインするときや送金操作時に、使い捨てのパスワードがスマホに送られて来て、これをパソコンからサイトに入力するとしましょう。

このとき、銀行のサイトだと思っていたものが偽サイトだとしたらどうなるでしょう。攻撃者が、私たちが偽サイトに入力した内容を本物のサイトに中継して、画面の内容をリアルタイムに模倣していたとしても、気付かないまま送金の操作をしてしまうでしょう。

攻撃者が通信を中継しながら、送金先を別の銀行口座に差し替えていたら、二要素認証を使っていても不正に送金されてしまいます。

このような、通信経路の中間で双方の通信を中継しながら裏をかく手口は「中間者攻撃」と呼ばれています。たとえ多要素認証を採用していても、この中間者攻撃をすべて防ぐことはできません。

結局、偽サイトによる攻撃は、利用者自身で自分がどこのウェブサイトを見ているのか、注意して確認する以外に対策はありません。では、どのように注意すればよいのでしょうか。

本物のサイトが、前ページの図にあるようにEV-SSL証明書を使っている場合には、パスワードを入力する直前に、ウェブブラウザ画面のアドレスバーの鍵マークから証明書を表示して、自分の利用している企業や団体名や所在地とあっているか確認する方法もあります。

ただ、先ほど説明した通り、攻撃者が偽のSSL証明書を取得していることを考えると、鍵マークなどの有無だけでは判断できません。

また、アドレスバーのURLを見て自分が知っているウェブサイトとドメイン名が同じかを確認します。

「ドメイン名」とは、例えば「https://www.example.co.jp/foo/bar.html」のうち「example.co.jp」の部分のことです。

ただ、これを確認するのも簡単ではなく、攻撃者は利用者が見間違うのを狙って、「https://www.example.co.jp.foo/bar.html」という、似たURLで偽サイトをつくることがあります。このURLのドメイン名は「co.jp.foo」であり、「co.jp」とは全く違うところなのですが、「.」と「/」の違いを見抜けないと気がつきにくいのです。

最近のウェブブラウザでは、URL中のドメイン名部分がどこなのかを強調表示してくれるものや、アドレスバーにドメイン名部分しか表示しないようにしているウェブブラウザもありますので、そういうブラウザでは見分けがつきやすいでしょう。

その場合でも、URLの一部をアルファベットに似た別の言語の文字を使ってURLを偽装する手口もあります。

こう言った状況を総合的に鑑みると、自分が利用するウェブサービスは、基本的にあらかじめブックマークしておいて、訪れる際も、詐欺に用いられやすい偽サイトへの誘導に使われるメールやメッセージのリンクは利用せず、直接ブックマークから訪れるか、スマホの場合は公式のアプリを利用するのが安全でしょう。

もうひとつ注意したいのは、野良Wi-Fiや、公衆無線LANを利用する時に同名のSSIDに偽装した攻撃者のアクセスポイントに誤って接続してしまうケースです。安全でないアクセスポイント（P69の図で接続が×や△になっているもの）に接続している場合には、DNSハイジャックといって、通信経路を誘導する情報が改ざんされ、ブックマークから正規のサイトへ接続しようとして、ブラウザ上も正規のサイトに接続しているように見えても、偽サイトに誘導される場合があります。野良Wi-Fiや運営主体の分からない公衆無線

LAN、同名のSSIDのアクセスポイントがある場合の利用は避けるようにしましょう。

10 ウェブサイトを使ったサイバー攻撃に対応する

スマホやパソコンがマルウェアに感染したことによる、パスワードなどの情報流出。

事態が起こるまでには、マルウェアに感染する経路が必ずあり、それがウェブブラウザであることもよくあるケースです。最近では、ウェブブラウザでウェブサイトを「見る」だけで感染させる攻撃も発生しています。

攻撃者があなたに、マルウェアを仕込んだウェブサイトのURLをメールやアプリのメッセージで送り、あなたがリンクをクリックして悪意のあるウェブサイトを見てしまう場合（フィッシングメール）や、あなたの行動パターンを調べて、よくアクセスするウェブサイトに、事前にマルウェアを仕込んでおく水飲み場攻撃、さらにわざわざお金を払ってマルウェアが含まれた動画広告などを目的のウェブサイトに出すという方法（マルバタイジング）もあります。攻撃は不特定多数を対象に行われる場合もあります。とくに、広告を使うものは、攻撃者は広告費以上のお金を稼がなければならず、攻撃は無差別に不特定多数に対して行われ、被害者も大変多くなります。

この「見る」だけで感染するサイバー攻撃は、未知のセキュリティホールが突然狙われる場合もあるのですが、ネットでセキュリティホールが公表され、メーカーがそのソフトやアプリを修正するまでの「穴が開いたまま」の期間を狙って攻撃する「ゼロデイ攻撃」で行われる場合も多くあります。

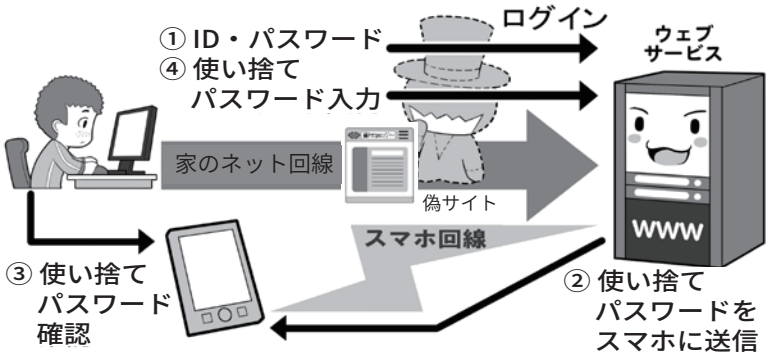
また、見るだけでなく、あなたの心の隙を突き、巧妙に誘導して「自らクリックやインストールさせる」といった攻撃もあり、この場合はセキュリティホールがなくても攻撃ができてしまいます。

なお、セキュリティホールを狙ったサイバー攻撃に対する基本の対策は、システムの状態を最新に保つことですが、セキュリティホールの修正など対応が間に合わない場合は、あなたが意識して攻撃を避けるほか対処法はありません。

さらに、利用者を巧妙にだましシステムのセキュリティ設定を変えさせて、自らアプリなどをインストールさせる攻撃に至っては、誰にでもある人間の心の隙を、自分が理解しなければ防げません。

そういった場合に備えて、「不審なメール文中のリンクは開かない」「なにかをインストールさせようとするものは拒否する」「ニュースなど情報を常時ウォッチして、特定のウェブサイトやアプリを使った攻撃が判明したらそのサイトやアプリに近づかない」「SNSやウェブサービスの動画や広告は自動再生しないように設定する」などの防御策を積み上げて守りましょう。

間に入ってなりすます中間者攻撃



中間者攻撃では、利用者とサーバの間に攻撃者の偽サイトが入ります。攻撃対策として二要素認証を使っていても、改ざんされた情報を見せられたまま処理が進むので、防御が意味をなさないこともあります。

ウェブを使ったサイバー攻撃の例

4 メールを安全に利用する、暗号化で守る

1 メールにおける暗号化

次は、メールを安全に使う方法についてです。

「ウェブを安全に利用する」の項目で書いたとおり、メールの送受信もすべての通信の中の一部です。

そして、メールの内容を盗聴されないためには、暗号化の区間が限定される無線LANの暗号化やVPNではなく、メールが送受信中常に暗号化していることが大切です。特に、メールはウェブと異なり、私的な内容が含まれるからです。

メールの送受信では、使用するスマホやパソコンなどのソフトやアプリから、メールサーバまで、送信と受信に別々の通信チャンネルを利用します。

2 送信の暗号化と受信の暗号化

メールは、昔はどちらも暗号化されていない平文で通信が行われており、送信を行うSMTPと呼ばれる通信が25番ポート、受信のうちPOPと呼ばれる通信が110番ポート、IMAPと呼ばれる通信が143番ポートを利用していました。

それが、後になって、平文でのメール送信による盗聴の危険性を回避するため、465番ポートを使って、SSL/TLSによる暗号化を組み合わせてSMTP over SSL（SMTPs）が普及しました。これと併せて、メール受信側の暗号化も普及し、POPがPOP over SSL（POPs：995番ポート）、IMAPがIMAP over SSL（IMAPs：993番ポート）で提供されるようになりました。

現在では、多くのプロバイダメール、携帯電話キャリアメール、フリーメールサービスで、この暗号化によるメール送受信サービスが標準になっています。

設定が「面倒くさくない」ように、スマホなどでは工夫されていて気付きませんが、最近では、特に意識しなくても自動的に暗号化で通信を行うようになっています。

一方、パソコンのメールソフトでは、依然として手動での設定が必要な場合もあるので、パソコンメールを使っている人は一度、自分のメールソフトのメール送受信サーバの設定がきちんと上記の暗号化ポートや類似の方式を利用しているか、もしくはSSL/TLSなどの文字がある設定になっているかをチェックしてみてください。

特に、パソコンで古くからメールを利用し、メールソフトの設定を全然いじっていない場合、暗号化されていない昔の設定のままになっていることもあります。

多くのメールアカウントを持っている人は、一度メールアカウントの棚卸（たなおろし）をし、暗号化されていない設定があれば、暗号化した方式に切り替え、暗号化した方式がないものしか提供されていないメールサービスは安全でないと考え、安全なメールサービスに乗り換えるようにしましょう。

3 メールにおける暗号化の守備範囲

先ほども少し触れましたが、メール送受信の暗号化は、スマホやパソコンのソフトやアプリなどから、送受信用のメールサーバまでの間を暗号化します。

しかし、目的のウェブサイトの情報を直接閲覧するのと異なり、メールの送受信は自分が利用しているメールサーバから相手のメールサーバまで、複数の中継メールサーバによってバケツリレーのように、受け渡しによる送受信が行われる場合があります。

遠方の誰かに手紙を送ると、複数の郵便局を転送された後に、相手に配達されるのに似ています。

そして、残念ながら、このバケツリレー中の送信はいまだ平文で行われていることもあるのです。

自分や相手が契約しているメールサーバまでの経路をそれぞれ暗号化しても、その先のバケツリレーの区間で平文での送信が行われていれば、内容を盗聴されてしまったり、改ざんされてしまったりする可能性が残ります。

とはいえ、この転送中の通信の暗号化は、大手メールサービス提供会社の努力により進み、改善されつつあります。

ただ、途中の経路をすべて暗号化しても、それぞれのメールサーバで一旦暗号化が解かれますので、バケツリレーの途中のメールサーバに盗聴しようとする攻撃者がい

たら、内容を読まれてしまう余地があります。

現代でも外国に郵便を送ると、国や地域によっては手紙が開封されて中を見られてしまったりすることがあり得るのに似ています。通信の秘密が保障されるかは、国や地域によるからです。

それを避けたい場合は、安全な国内だけで手紙をやり取りするように、メール送受信を暗号化したサービスの中だけでやり取りする方法もあります。

4 メール本文の暗号化

ところで、メールの暗号化には、送受信の暗号化ではなく、メールの本文そのものを暗号化する手段もあります。

これには、「S/MIME」や「PGP」という方法があります。これらの方法を使うと、メールのバケツリレーの途中で攻撃者が盗み見しようとしても、そもそも本文が暗号化されているため読めません。

メール本文の暗号化には、公開鍵暗号方式の「公開鍵」と「秘密鍵」を使います。この方法を使うときは、事前の準備として、自分用の秘密鍵と公開鍵を作成しておく必要があります。

相手が自分の「公開鍵」で暗号化したメールを、受信して復号するには自分の「秘密鍵」を使い、相手にメールを送る際は相手の「公開鍵」で暗号化して送信します。

そして、これを成立させるためには、お互いの公開鍵を安全かつ確実な方法で交換しておく必要があります。

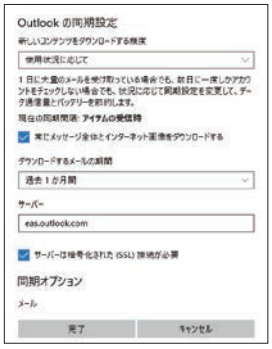
特に、S/MIMEを使う場合は、お金を払い認証局が発行する証明

メールの送受信は暗号化されているか

メールソフトやアプリが暗号(SSL/TLS)利用することになっているか？

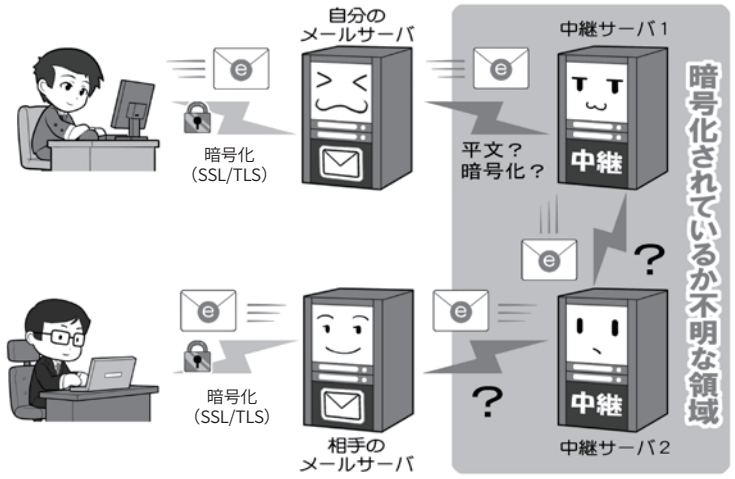
メールソフトの例

メールアプリの例



メールアカウントが設定された状態で、メールソフトやメールアプリの、サーバの詳細設定画面を開き、暗号化を利用する設定になっているかを確認します。「受信ポート 587 や 993 の使用」「送信ポート 465 の使用」「パラメータとして SSL 使用が ON」などになっているかがチェックポイントです。これらは暗号化通信が設定されている目印です。

しかしSSLの通信は自分のサーバまで



メールの暗号化設定は、利用者の機器から契約しているサーバまでの区間のみの暗号化が担保され、メールが送信相手の利用しているサーバに到達するまで経路は担保されておらず、平文で送信される区間がある可能性が残ります。

暗号化している同じサービスを利用する

メールを安全に利用する一つの方法としては、暗号化通信を採用した一つのメールサービスを、送信相手とともに利用する方法があります。通信の秘密が守られる国内だけで手紙をやり取りするのと同じ概念です。

書を入手し、自分の公開鍵の正当性を証明する必要があります。事前の準備も必要で、相手も同じことをする必要があるので負担にもなります。

なお、メールの本文を暗号化しても、メールのヘッダ部分、つまり、件名部分や、宛先と差出人のアドレスなどは、平文で送られることになるので、注意が必要です。

S/MIME や PGP を使うと、盗聴を防ぐことができるだけでなく、仮にメールの本文が改ざんされても、受信者側で改ざんの有無を調べることができるようになります。また、他人がなりすました偽のメールではないかを確認することもできます。これを実現する機能を「デジタル署名」と呼びます。

上記のとおり S/MIME は大変優れた機能なのですが、事前の準備に手間がかかり、また、大手のメールソフトが対応してないものもあって、残念ながらあまり利用されていません。詳しい方法の説明はここでは省略しますので、各自で調べてみましょう。

一方、利用者ではなくメールサービス側で成りすましを防ぐものとして、認証チェックをする SPF、DKIM、そして、これに引っかかった場合の対処を決める DMARC などがあります。これは、送信者の書面上のメールアドレスと実際にメールが発信されたサーバのドメインをつきあわせて、合っていなければメールを受け取らないなどの対応ができるものです。これらを採用したメールサービスがあれば、積極的に利用を検討してもいいでしょう。それが安全な技術の普及への一助になります。

5 怪しいメールとはなにか

メールを安全に使うために、メールを使ったサイバー攻撃にも触れておきましょう。

サイバーセキュリティの標語などでは、よく「怪しいメールを不用意に開かないように」といったものを見ます。これは、「標的型メール攻撃」に代表されるフィッシング（詐欺）メールを使った攻撃に関する注意喚起をしています。この攻撃は、攻撃者が特定の個人を狙って仕事などのメールを装い、マルウェアの添付や、マルウェアを仕込んだウェブサイトのリンクを送り付けるものです。相手が添付ファイルやリンクを不用意に開くと「ゼロデイ攻撃」などを受け、不正なプログラムをインストールされたり、パソコンなどを乗っ取られたりするのです。

実際には、特定の個人を狙った標的型攻撃だけでなく、不特定多数を狙った「スパムメール」でも同様の手口が使われます。誰でも攻撃対象になりうるわけです。

これらの手口は、昨今のセキュリティ環境の向上で「開くだけ」「見るだけ」で感染させることが難しくなったため、少なくとも相手を「感染させるためになにがしかの行動を起こさせる」ことで感染率を上げています。それが、偽装したマルウェアをインストールさせたり、偽装サイトへのリンクをクリックさせたりする手法なのです。

こういった攻撃を避け、マルウェアなどに感染しないようにするためには、まず**「送られてきたメールの文面を見るだけで完結しないものは、すべて『怪しいメール』として警戒する」**ことが必要です。

送られてきたメールの差出人が知り合いでも、実は全く違う所から送られて来ていたり、あるいは間違いなく知っている相手から送られてきたメールでも、実は相手のパソコンが乗っ取られていて、そのパソコンから送ってきたりしていることもあります。知り合いからのメールだから安全とはいえないと覚えて下さい。

少なくとも、送られてくることが事前に知らされていない添付ファイルや、「今すぐ確認を！」といったように、緊急に文中の添付ファイルやリンクを開くことを要求するメールなどは、警戒する必要があります。次項目の偽装添付ファイルにも気をつけてください。

発信者に、送信されてきたメールについて「メールではなく電話などの別通信経路」で問合せをしたり、銀行・行政サービス・インターネットプロバイダ・サービスなどから送られてきた場合は、文中のリンクを開くのではなく、公式のウェブサイトやアプリを直接開き、本当に該当の情報が掲載されているかを確認し、もし個人情報に関わる問題であれば、ウェブサービス側に電話で問い合わせたりするなどの対応をしましょう。

6 マルウェア入りの添付ファイルに気をつける

「怪しいメール」の一つのパターンである、マルウェア入りの添付ファイルとはどういったものなのでしょう。

例を挙げると、業務を装ったメールに「報告書」などの一見文書ファイルなどに見える形で添付されるものや、ZIP ファイルというファ

イルを圧縮した形で添付されてくるものなどがあります。

そして実際は、こういったファイルは本当の文書などではなく、なんらかのマルウェアを含んだ不正なファイルであり、あなたがファイルをクリックして開くと感染するしかけになっています。

通常パソコンでは、ファイルはアイコンで表示され、アイコンには文書ファイルであれば文書ファイルを示す画像がつけられます。

しかし、このファイルのアイコンというものは、簡単に変更可能であり、文書ファイルに見せかけたマルウェアを作ることも可能で、事実そういった手法が使われます。

また、ファイル名は、文書ファイルであれば「文書名.doc」、ZIPファイルであれば「ファイル名.zip」というように、文書の名前の後ろに「拡張子」といって、そのファイルがどういった種類のファイルであるかを示す文字列が付け加えられます。(表示されていない場合は、ファイル拡張子を表示する設定に変更してください)

マルウェアが実行形式ファイル(プログラム)の場合、Windowsなら拡張子は「.exe」となり、exeと表示されれば「メールで実行形式ファイルが送られてくるのはおかしい」と気付く人もいます。

これを隠すために、攻撃者はファイルの名前を「houkokusyo.doc.....exe」というような長いファイル名にして、後半が省略され画面上で見えないように細工し、「houkokusyo.doc...」の部分だけが表示されるようにして、その上でアイコンを偽装するといったことを行います。

そういった手法に引っかからな

ウェブメールの送受信は暗号化されているか

ウェブブラウザでメールを送受信する場合は、ウェブブラウザの暗号化のチェック項目を参考にしてください。

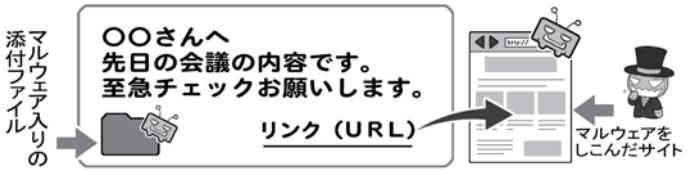
一般的には「SSL 証明書」や「EV-SSL 証明書」を持ち、暗号化通信を示す鍵マークがついていることで、暗号化されているかどうか、信頼性があるかどうかなどがわかります。

心配な場合は、パソコンなどでは鍵マークをクリックすることで、そのサーバを運営している主体を確認することができます。

安全性を確認をした上で、「ログインパスワード」などを入力します。

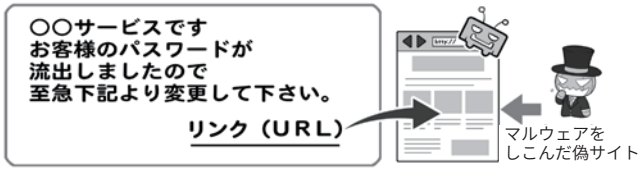
怪しいメールとはなにか

①仕事のメールを装う



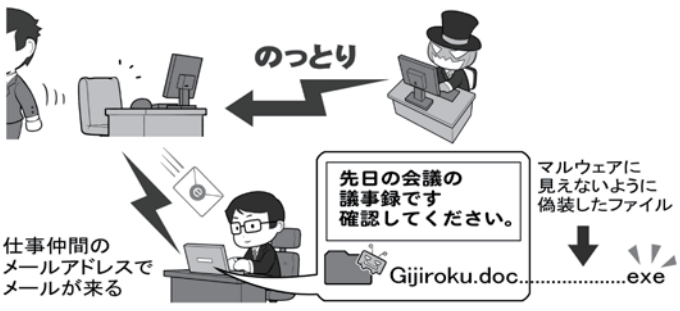
サイバー攻撃に使われる怪しいメールとは、まず「見ただけでは完結しない」メールです。リンクをクリックさせたり、添付ファイルを開かせたり、なにかをインストールさせようとしたりします。

②銀行、カード会社、オンラインショッピングサイト、プロバイダ関係を装うメール



また、自分が利用しているウェブサービスの名称で、緊急にどこかのウェブサイトを見させようとするのも、よく使われる手口です。

本当の仕事仲間のメールでも攻撃は来る



自分の知り合いや仕事仲間からのメールと思っても、安心はできません。なりすまして仕事仲間の名前を名乗っているだけでなく、攻撃者がその人のパソコンを乗っ取って、知り合いや仕事仲間の本物のメールソフトから攻撃をしかけてくることもあるからです。

いためにも、繰り返しになりますが、「送られてきたメールの文面を見るだけで完結せず、なにか行動させようとするメール」は、すべて「怪しいメール」として警戒することを心がけてください。

また、こういった攻撃手法は常にブラッシュアップされ進化していくので、定期的に検索エンジンやニュースなどで攻撃の手口を検索をして、最新の攻撃手法の情報を入手してください。

セキュリティソフトメーカーやフィッシング対策協議会、専門機関、識者などのSNSアカウントをフォローすると、最新の情報を入手しやすくなります。

7 メールアドレスのウェブサービスなどからの流出

「標的型メール」や「スパムメール」による攻撃には、送り先となるメールアドレスが必要です。

メールアドレスを、無差別に生成し送り付ける方法もありますが、ウェブサービスなどから流出した大量のメールアドレスを使って送られる場合も多くあります。

また、会社内で標的型メールによって感染した端末があると、そこから社内のメールアドレスが流出して、さらなる標的となる場合もあります。こういった情報は、攻撃者によって直接、攻撃メールの送付先として使われるだけではなく、インターネットの闇サイト（ダークウェブ）などで名簿として売買されることもあります。

攻撃のメールが送られてきたら、もちろん警戒するべきですが、それ以前にもできることがあります。

セキュリティ識者のトロイ・ハント氏が運営する、「Have I been pwned」というウェブサイトなどでは、メールアドレスやパスワードなどの流出情報を、すべてではないものの検索できるようになっており、そこで自分の情報が流出した形跡がないかを、ある程度チェックできるのです。

では、流出が判明したら、速やかに対処するのは当然として、流出に備えてメールアドレスにどのような工夫ができるのでしょうか。

8 流出・スパム対策としての、変更可能メールアドレスの利用

解決策としては、親しい人とやり取りをする大事なメールアドレスと、ウェブサービスや通信販売サイトなどに登録するメールアドレスを別にし、後者にはメールアドレスを気軽に変更・追加・削除したり、仮想メールアドレスが貰えるものを使う方法があります。

これは、「メールのサブアドレス」や「使い捨てメールアドレス」「捨てアド」と呼ばれるもので、ウェブサービスなどからメールアドレスが流出してしまっても、すぐに変更するかメールアドレスごと削除して、攻撃メールが送られてくるのを避けることができます。

思い入れがあり変えられないアドレスと違い、ウェブサービスなどに登録するアドレスは、すっぱりと変えたり捨てたりできるものを使いましょう。

一つのサービスからの流出によって、ほかのサービスに登録しているメールアドレスを変更するのが面倒なら、無限に近いサブアドレスを作れるサービスもあるので、それを利用してサービス毎に別々のアドレスを登録しましょう。

余談ですが、この方式でなら、攻撃者からスパムメールなどが来たときに、どのサービスから流出したかを知ることもできます。

なお、親しい人に限定して使っているアドレスでも、相手がマルウェアに感染して流出させる可能性もあります。さすがにその場合までは対処することができません。

ただ、逆に自分が流出させて迷惑をかけてしまう可能性もあるので、セキュリティを固め、自分から流出させないようにしましょう。

9 通信の安全と永続性を考えたSNSやメールの利用

メールの送受信での秘密を確保する手段として、送信者と受信者が「メールの送受信を暗号化している同じサービスを使う」方法について触れましたが、この「閉鎖された空間による安全性の確保」は、「すべての通信の暗号化を宣言しているSNSサービスを使ったメッセージのやり取り」にも当てはまります。

この場合、上記のメールサービスの利用と同じく、サービス全体が一つのセキュリティ方針で守られるので、安全性は確保されます。

ただし、SNSの運営企業によっては、すべての通信を暗号化しているかどうかを明確にしていない場合もあり、一般の利用者が自力で暗号化の状況を調べるのは容易ではありません。

現状では、検索エンジンで「自分が利用しているSNSの名前」＋「暗号化」などと入力して調べるか、暗号化を明言しているSNSサービ

スを選ぶしか方法がありません。本来であれば全SNSサービスが、暗号化とセキュリティの向上に対応してほしいところです。

この閉じた空間による安全性の確保は、確かに安全な通信に有効な手段である一方、様々な機器がつながりあって情報をやり取りする、「インターネット」の思想とは逆の発想でもあります。

本来は、多様なサーバがつながりあってバケツリレーが行われるメールであっても、すべての過程で暗号化が行われ、安全性が確保されることが理想なのです。

一方、現状では問題が残るメールですが、SNSと比較したメリットもあります。

メールは特定の企業サービスとは紐付かないインターネットの仕様なので、様々なメールソフトを使い、どのメールサーバに接続しても基本的には利用可能なのです。

一社によって提供され、栄枯盛衰（えいこせいすい）によってサービス終了する可能性があるSNSに対して、メールは永続性の点で有利といえます。

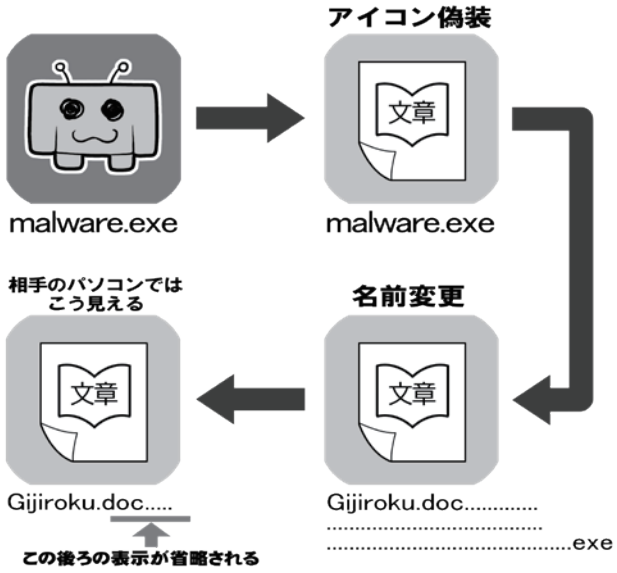
事実、インターネットの初期から様々なOSやメールソフトを乗り換えても、きちんとメールの内容を引き継ぎ、ごく初期のメールをきちんと見られる状況にしている人が少なからずいます。

SNSや各種通信サービスなどは、サービス終了時にデータのエクスポート(出力)の対応をすることもありますが、それらは保存されるデータであって、データが生きていた環境はサービス終了とともに終わってしまうわけです。その分、メールにはない、様々な華やかな機能を楽しむこともできます。

SNSとメール、どちらがいいかは人それぞれです。それぞれにメリットとデメリットがあるのでよく機能を理解して、自分に合ったものをうまく利用しましょう。

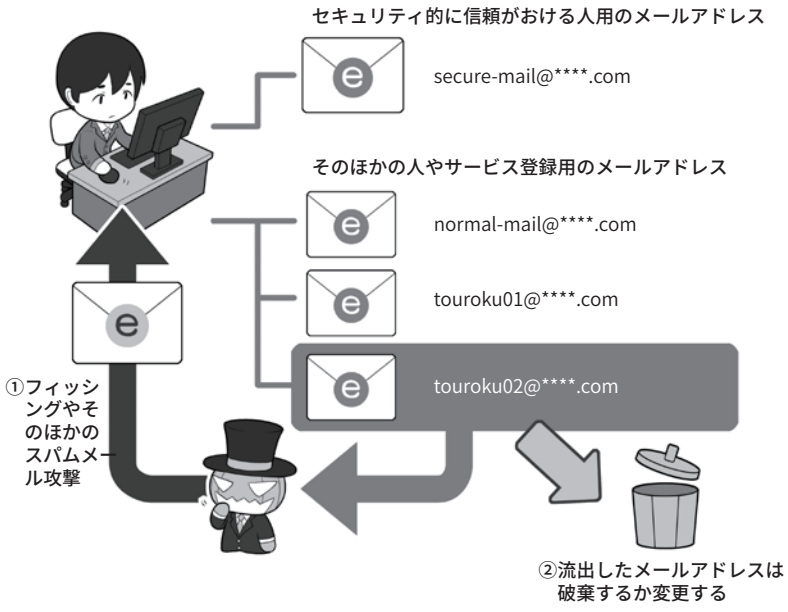
マルウェア入りファイルの偽装

マルウェア入りファイルの偽装



攻撃メールに添付されてくるファイルは、一見するとただの文章ファイルに見える場合もあります。しかし、ファイルのアイコンも名前も偽装したり、別のものに見せかけることは可能なのです

メールアドレスを変えてスパムメールから逃げる



メールアドレスの流出は、ウェブサービス側で管理しているものが攻撃者によって盗まれたり、ウェブサービス側の内部の人間が持ち出して売却したり、セキュリティ意識のない人がマルウェア感染して流出させることなどで起こります。愛着を持って長く使いたいメールアドレスは、むやみに人に教えたりウェブサービスに登録したりしないようにしましょう。流出してしまった場合に備えて、変更したり捨ててしまえるメールアドレスを活用しましょう。

5 データファイルを守る、暗号化で守る

もう一つ、通信にまつわる安全で考えなければならないのは「ファイルの暗号化」です。

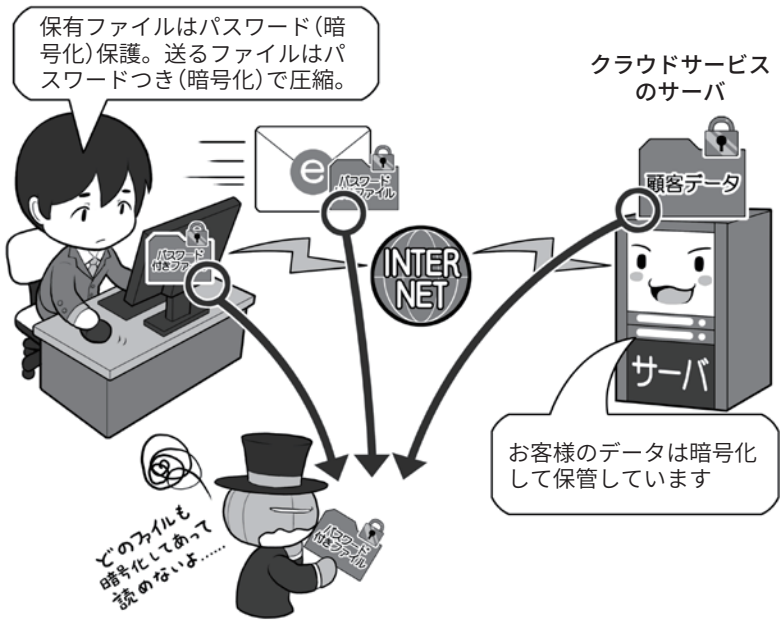
例えば、メールの添付ファイルが盗まれたり、保存しているファイルがマルウェアで流出したり、サーバに不正アクセスされて盗み見されても、また、ファイルの入った物理的な記録メディアを紛失しても、確実に適切な方法と鍵（暗号キー）で暗号化してあるならば、攻撃者が解読できなくなり、情報を流出から守ることができます。

ただ、ファイルの暗号化は攻撃者に盗まれると、高速なコンピュータを使って長い時間をかけて執拗に解読を試みられる可能性があります。「暗号キー」は基準にしたがって、長く複雑なものを設定しなければなりません。

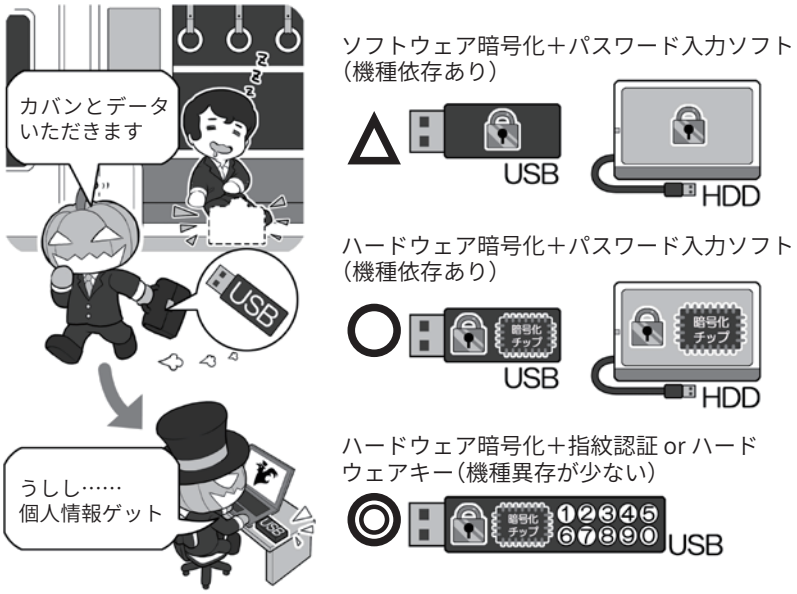
機密情報を持ち運ぶ場合は、ファイル単位の暗号化よりも、装置全体の暗号化機能が付いた外部記憶装置やUSBメモリの利用を推奨します。可能であれば、高速に暗号処理が可能で様々な攻撃に対策された暗号化チップが内蔵されたものを選択しましょう。そうすることで、ファイル単位の暗号化が不確実になった場合のトラブルも避けられます。

USBメモリの場合、汎用性と安全性を両立した、ハードウェアキーでパスワード認証をするタイプもあります。これらは、専用の認証ソフトウェアを必要としないので、利用するOSの依存度が少ないのと、ハードウェアキーの入力が「PINコード」と同じようになっており、入力を間違えると「ロック」や「データ消去」の保護機能があるほか、内部の「暗号キー」が十分に長く複

データの暗号化は保険



データを持ち運ぶときは必ず暗号化メディアを使う



＋「強制暗号化」＋「暗号化方式AES256bit以上」
＋「パスワード一定回数入力ミスで完全ロック（アクセス不能）」
あれば…「書き込み時ウイルスチェック（USBメモリ内機能）」

盗まれたメディアはリモートワイプができないので、より高度なセキュリティが求められます。しかし、それよりも重要情報を持ったまま飲酒したり、電車で寝たりすることは言語道断です。本来は暗号化よりもモラルが第一です。

雑なものが自動で生成され、この「暗号キー」の利用に「PIN コード」の入力を求めることで安全性を確保しています。

データの暗号化で重要になってくるのは「暗号キー」の運用です。

「暗号キー」は、英大文字小文字＋数字＋記号で、完全にランダムな15桁以上を基準としていますが、完全にランダムな場合、暗記することは困難になりますし、また、スマホのパスワード管理ソフトやパスワードノートを見て打ち込むのも一苦労になります。

かといって、パソコン上に保存したり付箋で貼っていたりすると「パスワードを利用場所に保管しない」というセオリーに反します。

現状は、単純で楽な解決方法はありません。ただ、暗記を前提にするのであれば、自分だけが知っているマイナーな曲の歌詞などからローマ字打ちで15桁よりかなり長くなる部分を抜き出し、一部を独自のルールで記号や数字に置き換えるなどの対策が考えられます。

また、暗号化したファイルを誰かとメールで受け渡しする場合、相手と「暗号キー」を共有する方法にも気をつけなければなりません。

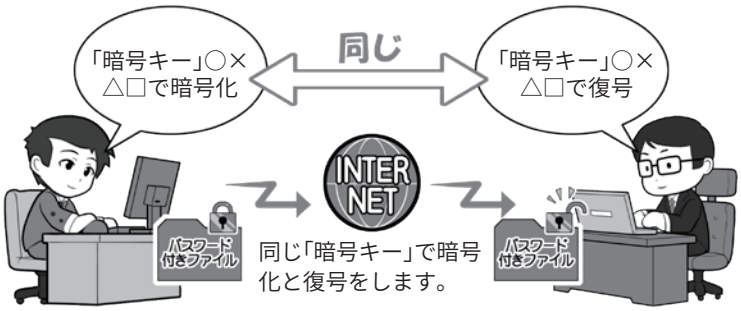
別送信であっても、暗号化ファイルと「暗号キー」を同じメールアドレスに送れば、メールが流出すると２つが揃ってしまいます。

「暗号キー」はメールでは送信せず、現実に会ったときに決めておくか、それができず、出先で突発的に送信が必要になった場合は、電話などで伝達するか、通信が暗号化されている「別系統の送信経路」で送るようにしましょう。

また、「暗号キー」には先ほども少し登場した、対になった２つの暗号キー（公開鍵と秘密鍵）を使ってやりとりする方式（公開鍵暗号方式）があります。この鍵は手で入力するのではなくパソコンが自動的に使うためのものですので、直接目にすることはないかもしれません。

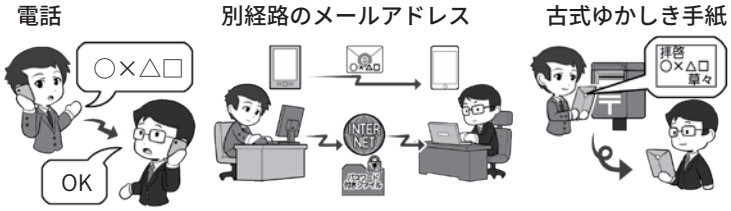
この方式を利用している具体例としては、P79 で紹介した「S/MIME」や「PGP」や、同じように目にすることはありませんが、Wi-Fi 通信の暗号化などがあります。

「暗号キー」が１個の方式（共通鍵暗号方式）



同じ「暗号キー」で暗号化と復号をします。

安全な「暗号キー」の受け渡しの例



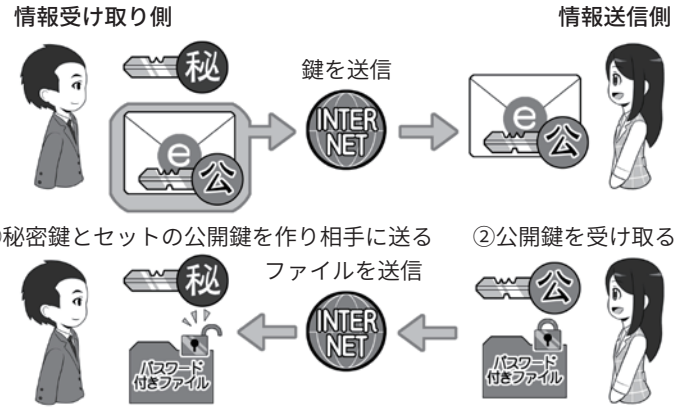
直接会ったときに「暗号キー」を渡したり、電話で直接伝えたりします。

盗聴やマルウェア感染を考え、スマホ対スマホなど別経路で送信します。

アナログだが一つの方法で、銀行などが利用しています。

どの場合であっても「暗号キー」の秘匿が重要です。

「暗号キー」が２個の方式（公開鍵暗号方式）



共通鍵暗号方式と異なり、「暗号キー」を送信しても大丈夫なのがポイントです。この方式では、「暗号キー」は手入力では使いません。メール送受信の影で使われていたりします。

コラム：究極の防御手段「ネットにつながない」エアギャップ

小さな会社の仕事などで、業務上どうしても個人情報などの入った顧客データベースを管理しなければならないが、マルウェアによる感染は怖いし、セキュリティを固められているか自信がない。

そんなときは、重要な情報の入ったパソコンを、極力ネットにつながずスタンドアロンパソコンとして使用するという手があります。

このネットにつながっているパソコンとスタンドアロンのパソコンの間、マルウェアが電子的に越えることができない壁を「エアギャップ（空気の隙間）」と呼び、立派な防御手段の一つとなっています。

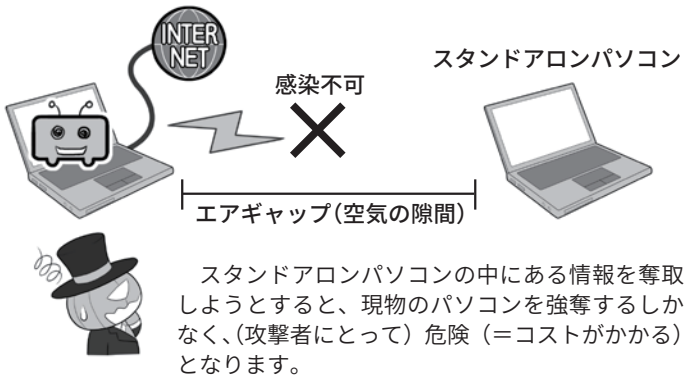
もし攻撃者が、このスタンドアロンのパソコンに入っているデータが欲しければ、物理的に事務所に忍び込まなければならず、それは、攻撃者にとって危険でコストがかかることであり、抑止力になるわけです。

ただ、データの盗難目的ではなく、破壊などが目的のマルウェアの場合は、USBメモリを介して感染させるという手法があります。それらを避けるには、きちんと管理できる人間以外がうかつにUSBメモリを挿せないように、パソコン側に鍵つきのUSB端子キャップなどを使いましょう。

余談ですが、この方式の場合、スタンドアロンパソコンが仮に感染しても、外部との通信ができないためデータの持ち出しは困難なのですが、パソコン内でのわかりきった場所にある少量の情報であれば、光るもの（LEDやパソコンのモニタ）、音、消費電圧の上下などを使って、外に向かって信号を送ることは可能であり、攻撃者がこれを観測できれば情報の奪取も可能となります。要するにこれらのものを使ってモールス信号を打つといわれればイメージがわくでしょうか。

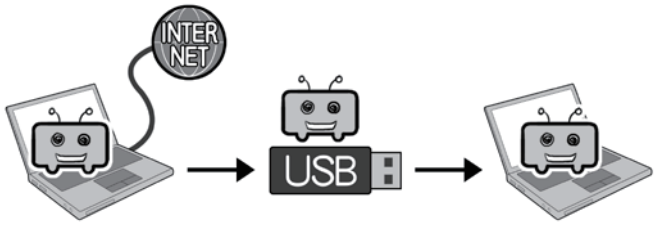
話題を戻して、エアギャップをインターネットバンキン

有線でも無線でも、つながっていないパソコンにはマルウェアは感染しない



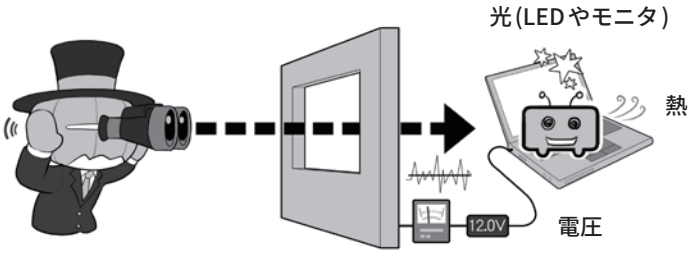
スタンドアロンパソコンの中にある情報を奪取しようとすると、現物のパソコンを強奪するしかなく、（攻撃者にとって）危険（＝コストがかかる）となります。

しかし、USBメモリを介して感染することも



かつて、イランで核燃料施設にあるスタンドアロンパソコンを感染させ、機器を暴走させた手法（Stuxnet型）です。ただし、攻撃者がマルウェアをネット経由で直接操作できないのと、データを抜き出すのは困難なマルウェアです。

ネットに接続していなくても、少量のデータであれば盗める



Stuxnet型で感染したパソコンに、あらかじめ特定のデータの内容を、デジタル信号の形で、光、音、電圧差などを使って発信させることは可能です。それを受信することができれば情報の奪取も可能です。ただし、通信速度は遅いので大容量のデータを盗み出すことは困難です。

グの不正送金の例に当てはめてみましょう。

インターネットバンキングのセキュリティの向上と、攻撃者の技術向上はいたちごっこであり、銀行などによって様々なセキュリティ対策が講じられますが、絶対に安全ということはありませんし、今後も難しいでしょう。

それは、攻撃者との技術競争的な問題もありますが、セキュリティに人間の心の隙という防御しにくい要素が含まれていることと、攻撃者がネットの闇に姿を潜めていて、現実世界でそこまでたどり着き、相手を捕まえることが容易ではないからです。

このうち、人間の心の隙に関しては一朝一夕に対策を講じることは難しいのですが、攻撃者がネットの闇から出てこなくてはならない方法で防ぐ手段はあります。すごくシンプルな方法でおどろくかもしれませんが、ようは取引をネットで行わなければいいだけなのです。

インターネットバンキングは確かに便利ですが、現在では、コンビニを含めあらゆる所にATMが設置され24時間稼働していますし、24時間送金可能なものもあります。したがって、多量の送金処理を毎日行うのでなければ、インターネットバンキングを使うのは「便利」ですが「必須」ではありません。

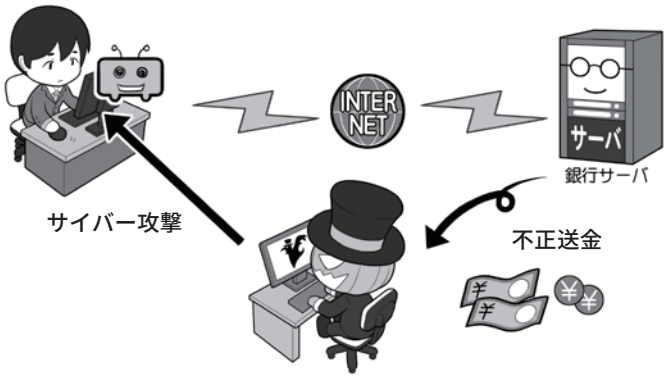
そして、ネットを利用しない場合、攻撃者が不正にお金を奪おうと思えば、現実世界でキャッシュカードとあなたの身柄を抑えて、暗証番号を聞き出さなければなりません。

そのようなことをすれば、当然のように顔もばれますし、リスク(コスト)も非常に高くなるので、攻撃者としてそういった手段は選びにくくなるでしょう。

このように、ときにはネットにつながない、ネットを利用しないという「ある種のエアギャップ」という選択肢をとることも防御の一つなのです。

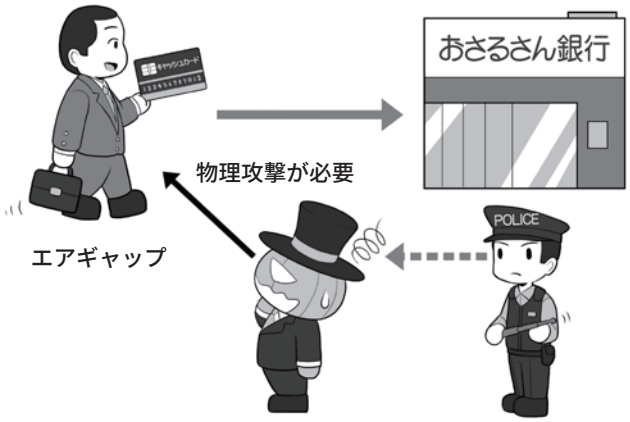
ネットにつなぐのは、「便利」の物差しだけで考えるのではなく、「利便性」と「危険性」を天秤の両側に乗せ、総合的に安全な選択肢をとるべきでしょう。

オンラインで銀行口座が狙われるなら



ネットを使って銀行口座から不正送金が行われるのは、そもそも送金処理をネットで行っていることと、攻撃者がネットの闇に潜んでいて、世界のどこにいるかわからず、検挙しにくいこともあります。

インターネットバンキングを止めるという手も



ネット経由ではなく、現実世界で送金処理を行うようにすると、当然ネットを使った不正送金はできませんし、お金を引き出す情報や鍵を持っているあなたと攻撃者の間には、エアギャップが存在することになります。無理矢理カードと暗証番号を手に入れようとすると、現実世界で窃盗や強盗をしなければならず、監視カメラなどにも映るので、リスク(コスト)がかかるようになります。このリスクが防御となるわけです。

コラム：「無料」ということの対価はなにか

インターネットでは、よく「無料」という言葉を見かけます。無料のメールサービス、無料のウェブサービス、無料の動画公開サービス、無料のアプリなどなど。

しかし、お店などの試食コーナーの図を見てもらうとわかりますが、私たち利用者の側から一見無料に見えても、サービスが提供されるときは必ず「コスト（費用）」がかかっています。そして、正常な企業であれば、コストが回収できないビジネスは行いません。そこにはなんらかの採算が取れるシステムが存在し、私たちが見えないところでお金が回って提供されているわけです。

その方法の一つは、広告による収益モデルです。広告主がウェブなどに広告バナーを出し、サービス会社はそれを資金源に運営するわけです。

広告システムがもう少し進むと、ウェブサービス会社が私たちのウェブ上での行動パターンや、趣味や属性などの情報を収集し、一見匿名の情報の形にして、これを広告主に提供、広告主は自社製品にマッチした人物向けに絞り込んで広告を打つなどして、より効果的な宣伝を行います。

このパターンでは、匿名とはいえ平たくいえば「私たちの情報」がサービスの対価として支払われているわけです。

また、先行投資といって、当初無料で提供し、サービスに馴染んだら、その後有料化してコストを回収するマネタイズを行う型もあります。

そして、最後にもっとも気をつけたいのが善意の無料サービスです。誰かがウェブサービスやアプリなどを開発し無料で提供するのですが、明示

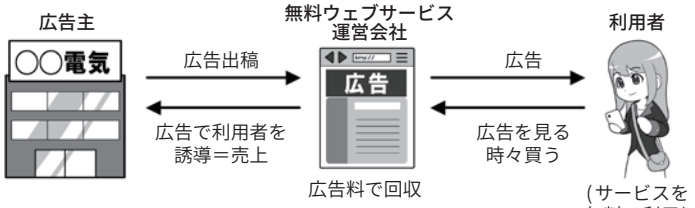
試食サービスのコストの例

（ソーセージを売る場合）

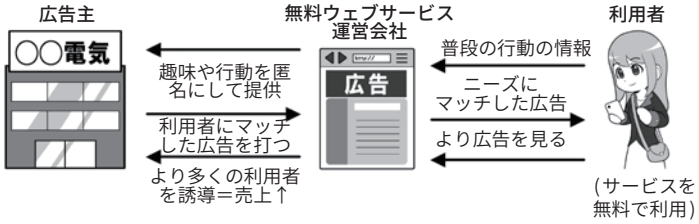
・食べる側は一見無料だが、人件費、光熱費、材料費は必ず発生し、どこかで誰かが必ず支払っている
・お店全体の売上や直接的なソーセージの売上の一部としてなど
・運営主体もしっかりして、コストも回っているので食べても大丈夫

無料ウェブサービスの例

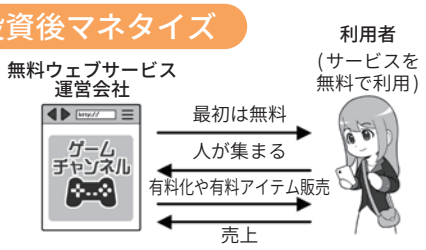
①無差別広告で運営



②利用者の情報を利用し、ターゲットに合わせた広告で運営



③先行投資後マネタイズ



④善意の無料サービス（ただし責任能力なし）

的ではなくても「責任は一切取りませんよ」という状態のものです。この場合コストは、提供する側のポケットマネーなどでまかなわれ、ビジネスとしては成立していないので、セキュリティに対して割くべきコストや労力がおろそかになりがちです。そして、ここが弱点として攻撃者に狙われ、利用される可能性があるわけです。

公衆無線LANの無料サービスの例も考えてみましょう。

政府機関・施設や自治体などが提供するものは、運営費とセキュリティの費用が、実は税金でまかなわれています。

携帯電話会社が提供する場合は、支払料金の中からまかなわれているので「追加料金無料」といった方がいいでしょう。

対価を払って利用する場合は、当然その支払料金が運営管理費用やセキュリティ費用にあてられます。

今回も問題なのは、「善意の無料サービス（ただし責任能力なし）」です。

小さなお店などで無線LANが提供されている場合、それは、仕事用のものを開放しているだけかもしれません。そして、無料で使っている以上利用者とは契約関係もなく、安全性を求める権利もないわけです。

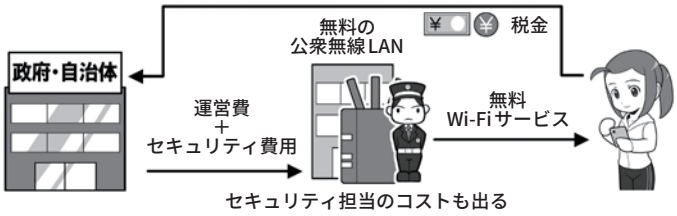
攻撃者は、このような所を狙って罠をしかけてきます。運営費もセキュリティ費用もないならば、誰も日常的に攻撃者の有無をチェックしないからです。

このような理由があるので、「運営主体がはっきりしていない、責任能力の無い無料の公衆無線LANは使用しない方がいい」というわけです。

無料という言葉には注意。費用の出所がはっきりしない場合、あなたが個人として高いツケを払わされることになるかもしれませんよ。

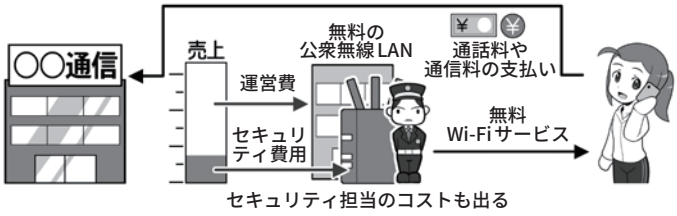
無料の公衆無線LANサービスの例

①一見無料だが税金などでまかなっているから無料



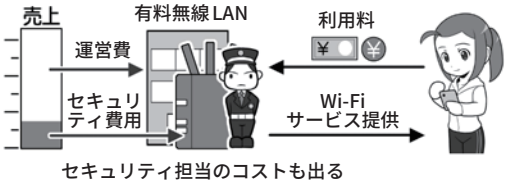
トラブルがあると議会などで取りあげられ問題となることもあります。責任能力もあります。

②企業が収入の中から払っているから（追加料金）無料



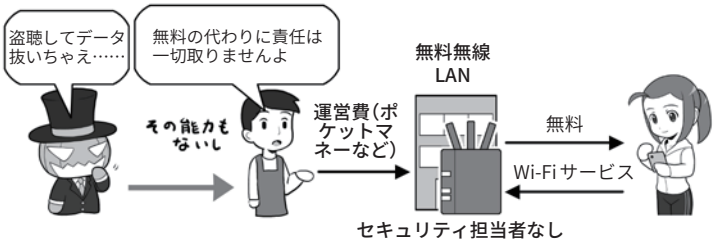
トラブルが起きれば責任問題となり、本業にも影響が出ます。責任能力もあります。

③対価を支払って利用する（有料）



対価をもらったサービスなので、トラブルが起きれば責任問題となります。

④善意の無料サービス（ただし責任能力なし）



対価はもらっていないので、トラブルは自己責任といわれたり、実質的に責任はとってもらえません（その能力もありません）。

コラム：クラウドサービスからのデータ流出。原因は？

クラウドサービスとは、「従来自分の手元で保存していたデータなどを、インターネット上のどこかに雲のように存在しているサーバに保存し、どの機器からでも、意識せず利用できる」サービスで、その雲的なイメージを指してクラウド（cloud）と呼ばれます。

実際には、サーバは雲や霞ではなく、どこかに歴然と存在していますし、概念自体は昔から存在するので、「意識せずに使える」≒「便利である」ことをクラウド（雲）と例えたあたりが、ポピュラーになったポイントでしょう。

最近では、スマホを利用していると、意識しないうちに写真などがクラウドにバックアップされていることもあります。それに、ウェブブラウザがあればどこからでもアクセスできるメールサービスも、クラウドの利用ともいえます。

パスワード管理アプリの記事では、クラウドサービスを利用することに関して厳しく書きましたが、クラウドサービスは、その性格を理解して利用するなら大変便利なものなのです。

一方、問題なのはクラウドサービスからの情報流出です。攻撃者がシステムを攻撃して大規模に情報を奪取することもないとはいいませんが、ニュースを賑わす話のほとんどは、利用者のパスワードが各種攻撃で破られ、クラウドから情報や写真を抜き取られたケースです。

ここでの攻撃とは、「リスト型攻撃」「辞書攻撃」、そして、個人情報からの推測などです。

ほかのサービスとIDとパスワードを使い回ししていて、侵入される場合もありますが、「パスワードは誕生日やニックネームから推測した」という攻撃者の証言もよくあります。

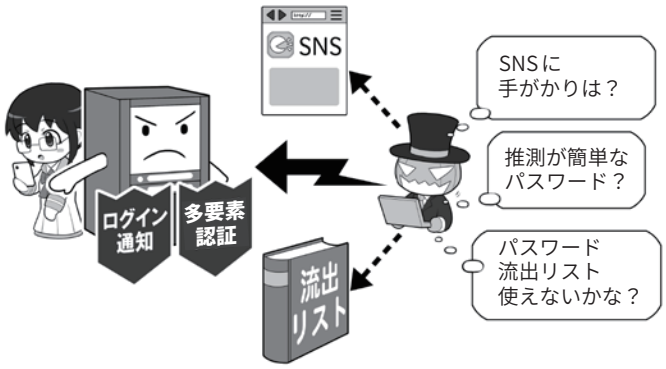
こういった流出事故を起こさないためには、まずIDとパスワードを使い回ししないこと。推測されるほど簡単なものにしないこと。多要素認証や、不正なアクセスがあった場合通知されるサービスを利用すること。そして、「流出して困る情報はクラウドサービスにアップロードしない・（自動で）されないようにする」ことです。

クラウドは大変便利ですが、きちんとセキュリティを固めなければ攻撃の的になると、理解して利用しましょう。

データはどこに保存されている？

スマホなどを使っていると、意識せずにクラウドサービスにデータをバックアップしていることもあります。よく分からない場合は、一度調べてみましょう。「クラウド」という名前ではなく、それぞれのサービス毎の名前をつけられている場合もあります。

パスワードが甘いと流出するかも



攻撃者は、クラウドサービスのパスワードを破るために、様々な攻撃を試みます。「ログインパスワード」の基準でパスワードを設定するなど基本を守るとともに、使い回しをせず、多要素認証の設定や不正なログイン通知を受け取れる設定を活用しましょう。