第5章

パスワードの大切さを知り、通信の安全性を支える暗号化について学ぼう

インターネットを安全に利用するには適切なパスワード管理が不可欠です。また通信の安全性を保つには暗号化技術が役立っています。パスワード管理、知っておきたい暗号化の必要性やしくみを学びましょう。

1 パスワードを守ろう、パスワードで守ろう

2 安全な無線LANの利用を支える暗号化について学ぼう

3 安全なウェブサイトの利用を支える暗号化について学ぼう

4 安全なメールの利用を支える暗号化について学ぼう

5 安全なデータファイルの利用を支える暗号化について学ぼう

1 パスワードを守ろう、パスワードで守ろう

1.1 3種類の「パスワード」を理解する

パスワードの役割を担うものには、他に「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▶用語集P.179して、他人や攻撃者▶用語集P.182が読めないようにする、「暗号化と復号▶用語集P.187の鍵＝暗号キー▶用語集P.180」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。私たちは、機器やウェブ▶用語集P.180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、スマホのロック▶用語集P.189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▶用語集P.177、パスコード▶用語集P.186。通信事業者のネットワーク暗証番号▶用語集P.185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▶用語集P.177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▶用語集P.186、ログインパスワード▶用語集P.189）

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▶用語集P.179として単独で用いられるもの（ZIPファイル▶用語集P.179のパスワード、WordやExcel、PowerPointの保護パスワード、Wi-Fi▶用語集P.179機器の暗号化キー▶用語集P.180、暗号キー、パスフレーズ▶用語集P.186、セキュリティキー▶用語集P.183、ネットワークキー▶用語集P.186）

一口にパスワードといっても、上記のとおり、実にさまざまなものがあります。第1章3（P.31-P.33）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。

1.2 「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

第1章3（P.31）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」桁数が多い方が安全に資するとされていると説明しました。

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桁以上でよいとしています。

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）」▶用語集P.184と呼び、「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▶用語集P.182する（ワイプ▶用語集P.190）」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空く、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▶用語集P.177のログイン▶用語集P.189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▶用語集P.189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。

1.3 「暗号キー」に求められる複雑さ

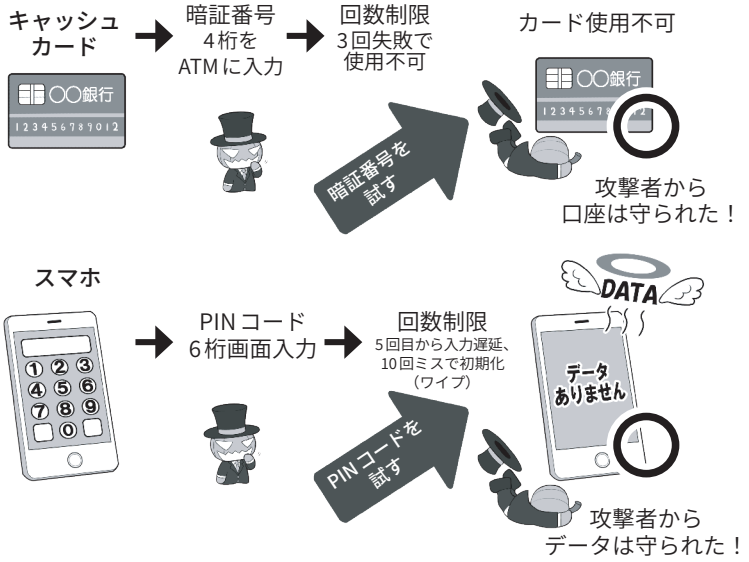
上記の「ログイン画面」に入力する「ログインパスワード」とは異なり、「暗号キー」の場合は、攻撃者が暗号化されたデータを盗んで持ち帰り、ログイン画面の遅延などなく、自分のペースで高速な暗号化解除（解読）の攻撃ができます。

この攻撃の対象となるのは、「1つ、または複数のファイルを圧縮したパスワード付き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▶用語集P.178メモリ」や「パソコンから取り出された内蔵補助記憶装置▶用語集P.181（ハードディスクやSSD▶用語集P.178。以下記憶装置▶用語集P.181）」、あるいは「暗号化された無線LAN通信の内容」などです。

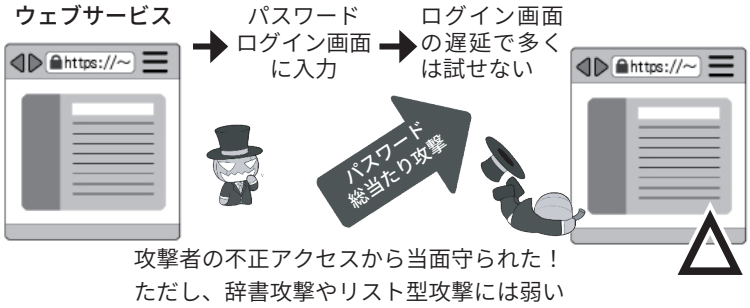
「暗号キー」が短いと、市販されているゲーム用パソコンの性能で暗号化解除は十分可能です。またこれらの性能が向上すれば、非常に短時間で解除されるような日がいずれ訪れても不思議ではありません。

3種のパスワードを理解する

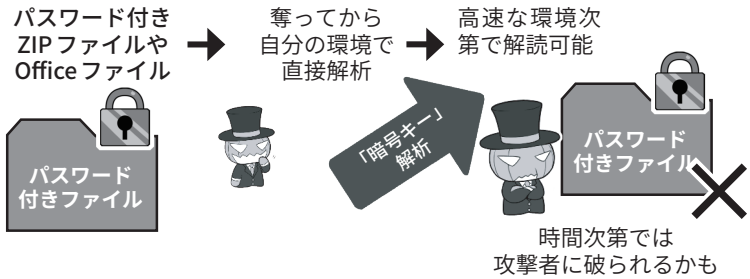
①「PINコード」の基準で安全性を保てる例



②「ログインパスワード」の基準で安全性を保てる例



③「暗号キー」の基準で安全性を保てる例

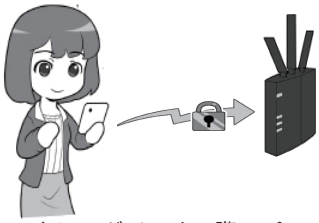


一見、安全性を保つための基準がわかりにくい例

内蔵記憶装置暗号化の救済が必要になる場面

「ログインパスワード」基準の複雑さで安全性を保てそうに思えるが、実際には入力遅延による防御が働かないので「暗号キー」の基準を採用すべき。

無線LANアクセス時に入力するパスワードを決める場面



ルータにログインする際のパスワードは「ログインパスワード」でよさそうだが、「暗号キー」の基準で設定した方がよい。

※この図は一例であり、実際の機器の条件とは異なります。

1.4 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」の他にもさまざまな手法があります。

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▶用語集 P.182（ディクショナリアタック▶用語集 P.185）」、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▶用語集 P.189（アカウントリスト攻撃・パスワードリスト攻撃▶用語集 P.186）」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、かつ他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▶用語集 P.182 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▶用語集 P.183」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」▶用語集 P.183 を利用するのも 1 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。

「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、本章「2 安全な無線 LAN を支える暗号化について学ぼう（P.110-P.117）」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

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

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

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）

1.5 多要素認証を活用する

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多要素認証▶用語集 P.184 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。

最も一般的な方法は、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▶用語集 P.190」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▶用語集 P.178 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▶用語集 P.179 を使って生成するソフトウェアトークン▶用語集 P.184 や専用の小さな乱数を発生するハードウェアトークン▶用語集 P.186 を利用する方法、そして物理的な USB セキュリティキー▶用語集 P.178 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なりすまし▶用語集 P.185 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▶用語集 P.178、または生体認証方式を推奨します。

生体認証は代表的な指紋認証のほか、目の虹彩▶用語集 P.182 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。

但し生体認証も 100% 安全とは言い切れません。最近では、どこかで撮影した相手の指や顔の写真から、3D プリンターや AI を用いて偽の指

紋などを作って認証を突破する実験もなされています。また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。したがって、生体認証だから、絶対安心と過信しないことが重要です。

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▶用語集P.186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▶用語集P.183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機種もあります。

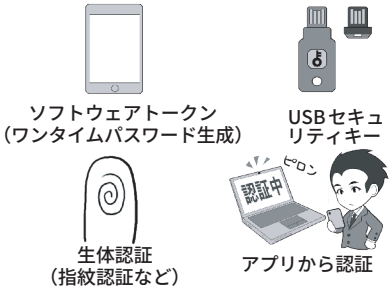
また、パスワードをネット経由で送信せず、USBセキュリティキーや生体認証を用いて端末内で本人確認をし、認証したという情報だけを送信するFIDO▶用語集P.176などの方式の採用も推進されています。より安全な利用のために、アンテナ高く認証にまつわるセキュリティ情報を収集しましょう。

1.6 二段階認証と二要素認証と多要素認証の安全性

この認証のために用いる要素には右図にあるように、「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。複数の要素を使用するものを多要素認証、その中でもとくに2つの要素を使用するものを二要素認証と呼びます。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。

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

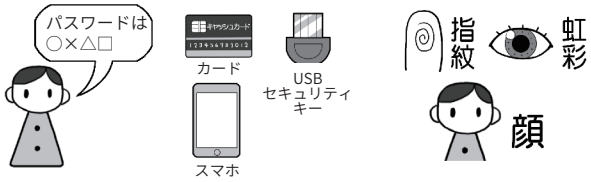


推奨できないもの

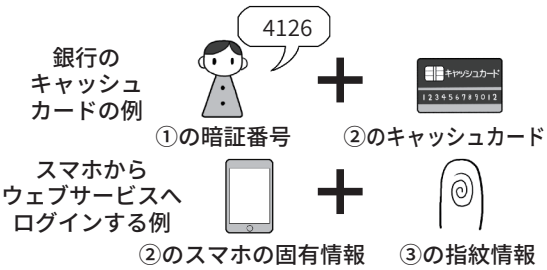
SMSを使ったワンタイムパスワード受信は、海外でSIMハイジャックという攻撃により破られた例があります。また、メールも同様にパスワードを「送信する」をいう点で攻撃の余地が多くなります。

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



多要素認証は上記の2つ以上の要素を組み合わせます

一方、二段階認証は、二回認証を行いますが、その要素は多要素とは限らないため、防御力としては弱くなります。

なお、多要素認証のうち、2つの要素だけ用いて認証するものを、「二要素認証」といいます。

指紋認証が破られることも…

極端な例ではありますが、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、強制的に生体認証ができない状態にする対策も検討しましょう。

一方、アカウント認証に関する記事などでよく用いられる言葉に「二段階認証」▶用語集P.185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。したがって、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、実物が必要という点で、安全性が高まります。

それでも、キャッシュカードが、振り込め詐欺などであっさり奪われたり、多要素認証すら破る「中間者攻撃」▶用語集 P.184（本章コラム3（P.121）参照）も存在したりするため、多要素認証だからそれだけで絶対安全とは限りません。

1.7 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た上で、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。企業などでパスワードに関するルールを定める場合にも、利用者に対して定期的な変更を求めないようにすることが原則として必要となります。

一方、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、その以降の被害を避けるため原因も特定しましょう。

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。

1.8 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▶用語集 P.180 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▶用語集 P.189 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。

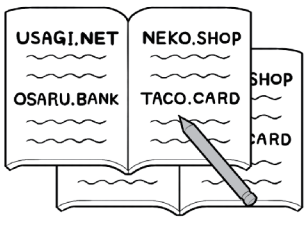
なお、ウェブサービスを利用するときは、パスワードが流出した場合に簡単にアカウントを乗っ取られないように、必ず二要素以上の多要素認証を設定しておきましょう。これが提供されないサービスは、セキュ

ウェブブラウザにはパスワードを保存しない

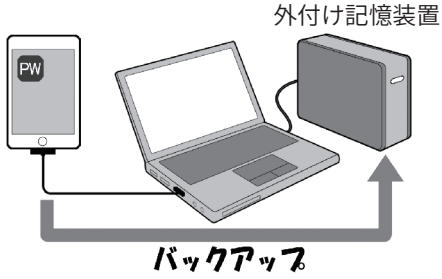
ウェブブラウザにパスワードを保存すると、席を離れた隙に勝手に利用されたり、パソコンをクラッキングされた際に根こそぎ盗まれる可能性があります。

パスワード管理方法の例

一見分かりにくい
紙のノートに二重で



管理アプリのデータは、暗号化した記憶装置にバックアップ



紙のノート二冊に記入したり、スマホのパスワード管理アプリを使って、パソコン経由で暗号化した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パスワードノートも売られています。

リティ意識が低い可能性があるのでそのサービスの利用は再考しましょう。

1.9 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。どう管理すればよいのでしょう。

パスワードの保管方法については、第1章「3.5 パスワードを適切に保管する」(P.33) でも示しましたが、ここではそれぞれの保管方法の特徴を紹介しましょう。

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▶用語集 P.186)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」▶用語集 P.183 状態で利用できるものを優先しましょう。

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し、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

パスワード管理アプリや、同様の機能を持つソフト▶用語集 P.184 には「クラウド連携機能」やクラウド▶用語集 P.181 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。またサービスとして提供されている以上、利用者が意図しない形でサービスが終了してしまうリスクもあります。

パスワード管理方法のメリットデメリット

	盗難・紛失対策	ネット経由のセキュリティ	データの管理者
 紙のノート	○ 持ち歩かず自宅などの安全な場所に保管する	○ 攻撃不可	本人
 スマホアプリ	△ 盗難・紛失のリスクが高め。バックアップが必要	△ 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、1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。

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がわからないことがあります。

クラウドサービスを利用する場合には上記のリスクを理解して、安全なものを選択する必要があります。

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。いずれの方法を採用した場合でも、その特徴を踏まえてリスクが小さく使いやすい形でバックアップを取ることが重要です。

1.10 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「ログインパスワード」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、別途パスワード管理を利用するのがいいでしょう(第1章 3.3(P.33) 参照)。また、これを解決する策として、「ソーシャルログイン」▶用語集 P.184 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、他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、グローバルで展開しているSNS▶用語集 P.178 サービスですら、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)が流出する事例はあるため、本書では、基本的にソーシャルログインを非推奨として、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。それらを活用し、パスワードの使い回し▶用語集 P.186をせず、ストレスなくルールを守るようにしましょう。

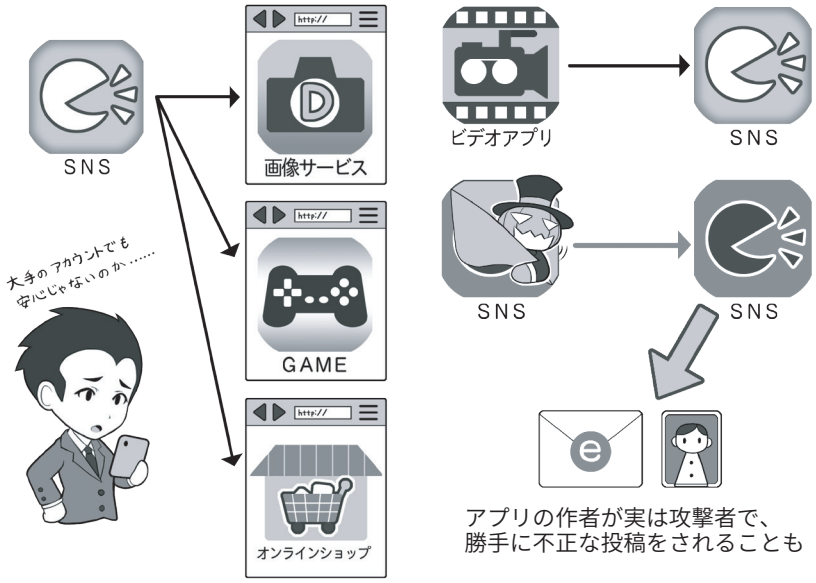
1.11 権限を与えるサービス連携にも注意

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」▶用語集 P.182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▶用語集 P.181を与える)」という部分が、攻撃者による攻撃の手段として利用されることもあり、また実際にメールアドレスや氏名が流出した例も存在しますので、利用する場合は気を付けましょう。

また、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、不要・不適切なものがないか、確認しましょう。

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。

コラム.1 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、その心配にはおよびません。

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。

使用する暗号化方式▶用語集P.180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。

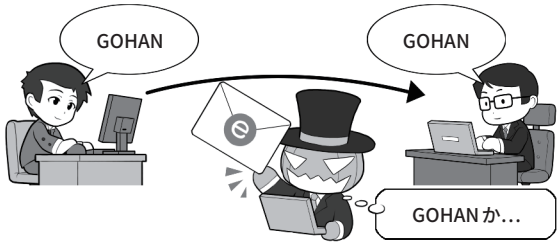
Cipher Disk(シーザー暗号)

最も原始的な暗号は、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。

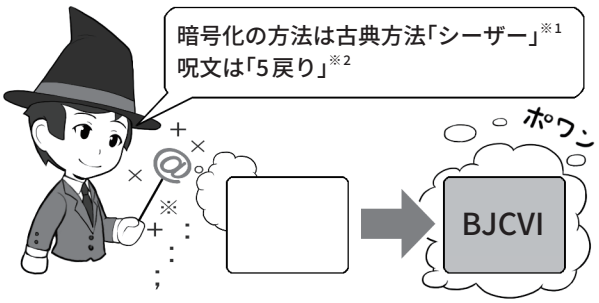
暗号化ってなに？

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

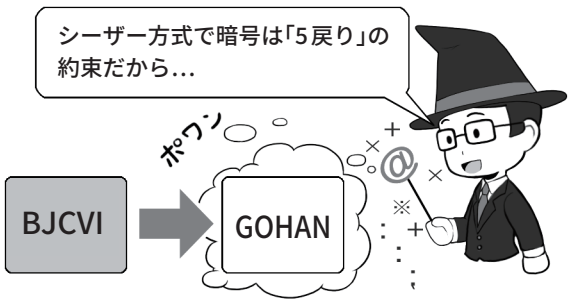


※1：暗号化方式　※2：「暗号キー」

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

コラム.2 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1つの対策だからです。

個人情報の流出は、最近では企業のサーバがランサムウェアの被害に遭い、これによる個人情報流出が挙げられます。このような流出事例は、小規模なものも含めると世界中で毎日のように生じており、事例を取り上げれば枚挙にいとまがありません。こうして流出したIDとパスワードは、必ずといってよいほど不正アクセス▶用語集P.187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1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▶用語集P.177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、ユーザーに厳格な運用を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。

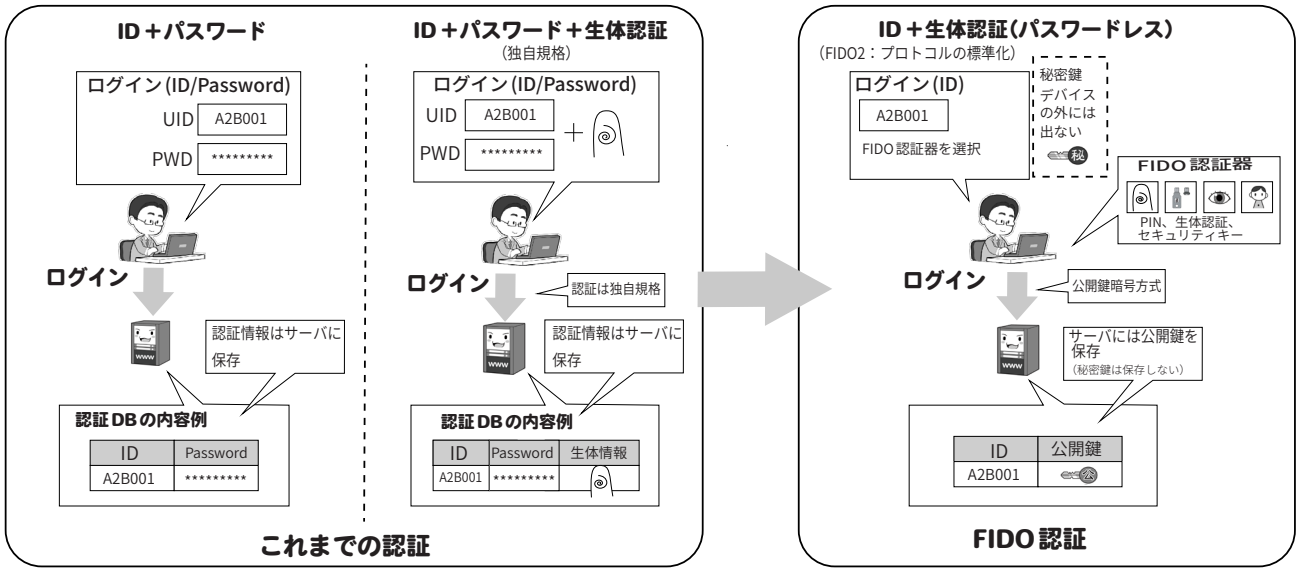
これを解決する方法として、第1章「3.5 パスワードを適切に保管する」(P.33)、本章「1.9 適切なパスワードの保管」(P.104)で紹介したように、パスワードをアプリや紙で管理することが有効です。特にパスワード管理アプリは、単にパスワードを保管してくれるだけではなく、条件を設定するとそれに合わせた長くて複雑なパスワードを自動的に生成してくれる他、最近では、ウェブブラウザでのサービスログイン時に、自動的に起動してIDとパスワードを入力したり、アプリ起動時にもIDとパスワードを入力してくれたりするように進化しているものもあります。

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▶用語集P.185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。このようなQRコードを読み込ませておけば、パスワード管理アプリがサービスごとの「ソフトウェアトークンアプリ」の代わりとして機能してくれるので、サービスごとにアプリを入れることなく、一括して管理できるため便利です。

■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をな

これまでの認証方法とFIDO認証の比較



※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。

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(Fast IDentity Online)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。

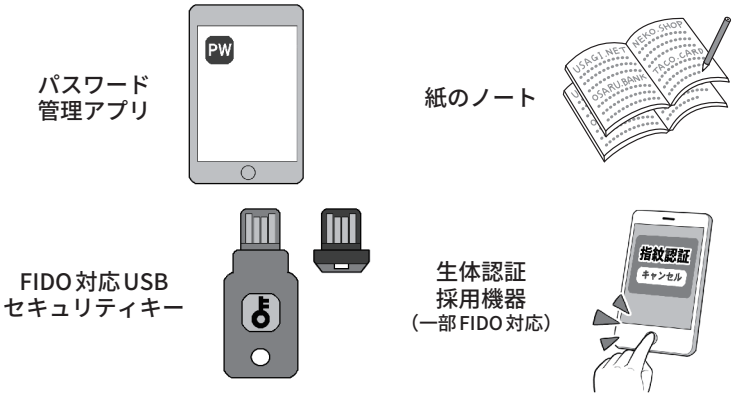
2022年12月にはFIDOアライアンスよりApple、Google、マイクロソフトなどのグローバルIT企業がFIDOの技術仕様を活用した「パスキー」というパスワードを使用しない認証方法を採用することが発表され、2023年12月時点で全世界で約70億以上のアカウントの認証に用いられている旨が公表されています。パスキーについては、NISTから2024年4月に公表された"SP 800-63B"の補遺で、フィッシング耐性など高度なセキュリティを求める一方で、ある程度の使いやすさも確保するレベルの認証方法である旨が示されています。パスキー対応のサイトやサービスは、わが国では携帯電話キャリアや携帯ゲームベンダー、その他グローバルIT企業での採用が進んでおり、FIDOの利用が大きく進展する可能性は高まっているといえるでしょう。

■パスワード流出が検知された場合

パスワードの流出は、登録しているサービスやブラウザ▶用語集P.188から側から流出の事実が通知されることがあります。例えば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他、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しています。このような通知があった場合、第三者からなりすまされたり、サービスの利用が乗っ取られたりする危険性が極めて高い状態にあると言えるので、速やかにパスワードの変更など対応するようにしましょう。特にパスワードを使いまわしている場合には、すぐにでも対応する必要があります。

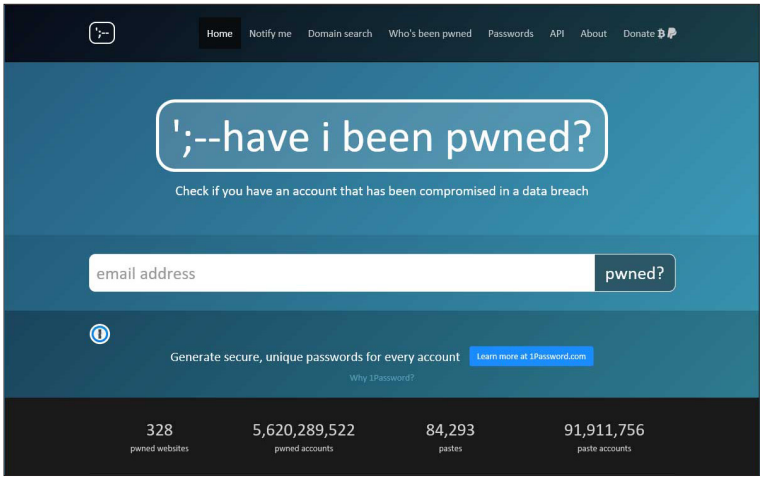
なお、他にも、例えば「Have I Been Pwned?」など、流出したIDとパスワード情報を収集し検索できる検索サイトもあります。必要に応じてこのようなサービスを利用することも一案です。ただし、信頼できるサイトでない場合には、かえってパスワードの流出を招く恐れもありますので、十分に留意して利用しましょう。

パスワード管理と認証の方法



パスワード管理アプリや、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。またネット接続しない紙のノートによるパスワード管理も、紛失・盗難に備えた上なら安全性は高いといえます。

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



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/

他にも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、その点を理解して必要に応じて利用することも一案です。

2 安全な無線LANの利用を支える暗号化について学ぼう

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内容や添付ファイル、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、さまざま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となります。

そもそもインターネットは、その始まりにおいて暗号化などが全くされておらず、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、世の常として悪意を持ったものたちが現れ、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。

2.1 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、さまざまな状況に合わせた、それぞれの暗号化があります。

私たちが通信すること1つをとっても、有線LAN、LTE▶用語集 P.177などの携帯電話回線、Wi-Fiなどの無線LANなど、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対象の1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、盗聴に際してとくになにか物理的な工作を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居るだけで、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▶用語集 P.188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、インターネット上に投稿されたあげく、世界中から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。

その対策をつぶさに挙げていくと数限りないのですが、このセクションでは、まず私たちの生活で最も身近な無線LAN通信の暗号化について説明しましょう。なお総務省では、ウェブページ「無線LAN（Wi-Fi）の安全な利用（セキュリティ確保）について」において、無線LANの利用のための簡易なマニュアル等を提供しています。

2.2 無線LAN通信（Wi-Fi）の構成要素

無線LAN▶用語集 P.188(Wi-Fi)による通信は、インターネットにつながった無線LANアクセスポイント▶用語集 P.189さえあれば、いちいちIT機器にLANケーブルをつながなくても、手軽にインターネットを利用できます。

会社で利用する無線LANでも、外出時に利用する公衆無線LAN▶用語集 P.182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知っておきましょう。

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」▶用語集 P.189、「Wi-Fi ルータ」▶用語集 P.179 あるいはシンプルに「ルータ」▶用語集 P.189」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)」▶用語集 P.178 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のパスワードのように使われる他、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 を利用できることを目的として、「00000JAPAN(ファイブゼロジャパン)」▶用語集 P.176 のように「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。

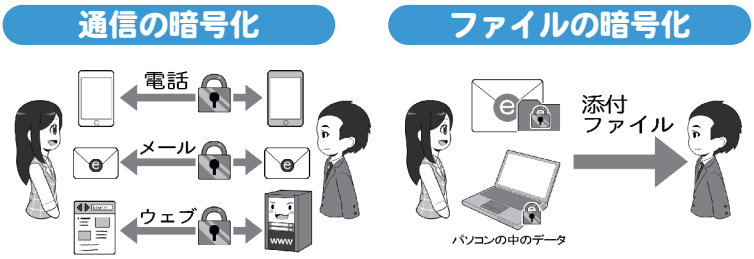
(その安全性は別として)この場合は利用時に暗号化方式の設定も「暗号キー」も必要ありません。

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」

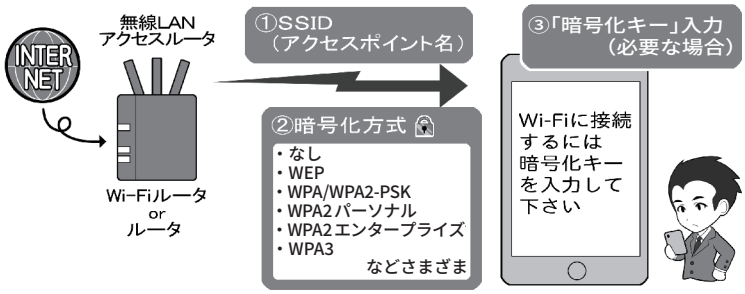
② 「暗号化の鍵(「暗号キー」)が公開か漏れている場合」

それぞれの状況に合わせた暗号化



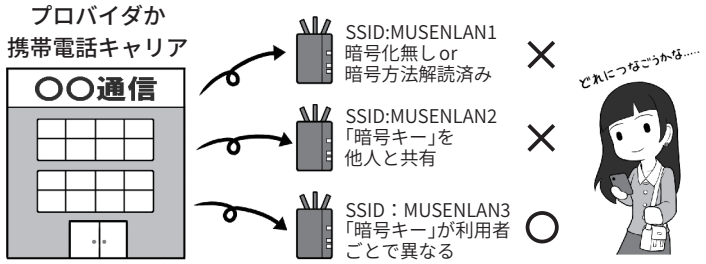
暗号化には、電話、メール、ウェブサイト閲覧などの「通信の暗号化」と、ファイルやパソコンの内部記憶装置などの「ファイルの暗号化」があります。

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、提供している公衆無線 LAN 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。

安全な通信をするために、自前で暗号化を行うテクニックがなければ利用してはいけません。

2.3 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、なんらかの別の手段での暗号化を行わないまま使っていると、攻撃者に盗聴され、即座に内容を知られてしまいます。

そのため、まず「暗号化無し」のアクセスポイント▶用語集 P.179 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「2.12 公衆無線 LAN が安全でない場合の利用方法」(P.116) 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、例えるなら拡声器を使って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るのです。

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、周りに居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」▶用語集 P.179 という名前のものや、方式の名称の中に「TKIP」▶用語集 P.178 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 ▶用語集 P.179-PSK (AES ▶用語集 P.176)、WPA2 ▶用語集 P.179-PSK (AES)、WPA2-EAP、WPA2- エンタープライズ、IEEE 802.1x、SIM 認証▶用語集 P.178、そして無線 LAN の多くの問題点を解決するために登場しつつある WPA3 ▶用語集 P.179、それらの記述があるものです。安全な方式の詳細は本章 2.9 (P.115) を参照してください。

2.4 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▶用語集 P.184 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、辞書が他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。

2.5 会社などでの安全な無線 LAN の設定 (暗号化方式)

会社などで無線 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) か WPA2-PSK (AES)、WPA3 を利用し、「暗号キー」を基準にしたがって、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「社員や会員だけが知っている」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「暗号キー」は関係者だけしか知らないものに変更しなければ安全が確保できません。

メーカーによっては「暗号キー」が同一機種で共通だったり、付け方に規則性があるかもしれないからです。

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、無線 LAN アクセスポイントの名前となる SSID を変更する場合、会社や団体の名前、社員や会員個々人を想起させる語句は使わないようにしましょう。会社や団体、もしくはあなたが攻撃の対象の場合、攻撃するべき無線 LAN が特定されるヒントになるからです。

家庭用無線 LAN アクセスルータには、標準で 2 つ以上の SSID を持てるものが多く、そのうちの 1 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、おも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設定できる SSID にし、安全でない昔の暗号化方式しか選べない場合は、利用を諦め買い換えましょう。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。

来客に社内用の SSID に接続させ

るのも安全ではありません。「暗号キー」が「社員・会員だけが知っている状態」では無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1つを来客専用にし、2つのアクセスポイント▶用語集 P.179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。

2.6 会社などでの安全な無線LANの設定(その他)

無線LANアクセスルータには、ウェブブラウザ▶用語集 P.180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であり、「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、もしルータのある場所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。

設定画面は無線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、建物外部の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原則、利用不可にしましょう。

UPnP(Universal Plug and Play)▶用語集 P.178の設定も、不用意に社内の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オフにします。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

会社内での無線LANの利用

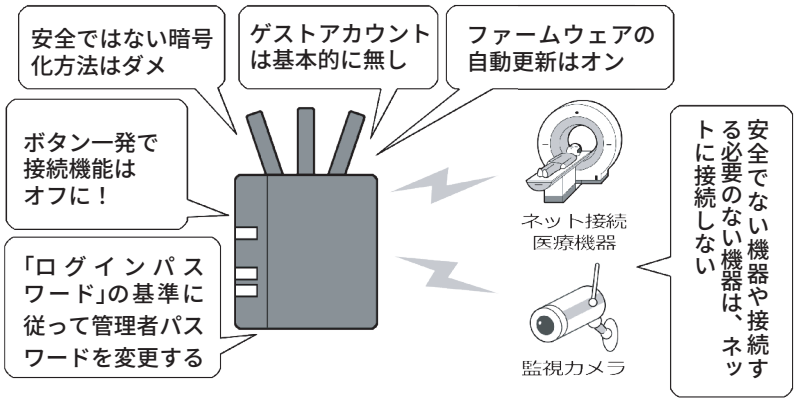
①出荷時の管理者パスワード、「暗号キー」の変更

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」は社員・会員だけの秘密

家庭で使える暗号化方式は、「暗号キー」を社員・会員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。部外者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



会社や団体で無線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LANに接続しないようにしましょう。

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▶用語集 P.187の自動アップデート▶用語集 P.179機能がある場合はオン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アラームを作り、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。

「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」については、現在では、これら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、社内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。また、どうしてもマルウェア感染が心配な場合は、「am I infected?」(https://amii.ynu.codes/)というサービスを利用すれば、現在使用中の機器が感染しているかどうかの確認ができます。

2.7 公衆無線LAN利用時の注意

公衆無線LANの安全な利用は、社内・団体内用の無線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、この方式では社内などの利用と同様に、複数の人が同じ「暗号キー」を使うことになります。

これを公衆無線LANにあてはめると、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。

その設定の状態で無線LAN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)を使った攻撃をしかけられ、盗聴される可能性を避けられません。

こういった危険なアクセスポイントを使用する場合、安全な暗号化方式の選択で安全性を確保する方法と、これとは別の暗号化機能で対処する方法があります。

なお、無料の無線LANを接続する際に、自分のメールアドレスやSNSのアカウントの入力を求め、それらに認証のためのURL▶用語集 P.178を送付して、無線LANの利用者が、メールアドレスやSNSを利用する本人であることを確認する方法もあります。ただし、これによる本人の認証は、結局、メールアドレスやSNSの取得に際しての確からしさに依存するほか、利用する無線LANの暗号化レベルとは直接関係がないので、利用の可否の判断にはあまり影響はありません。

2.8 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。最近ではWPA2に代わって新しい規格であるWPA3を利用するものもあります。

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ます。

利用前にそのページをチェックし、上記の暗号化方式のキーワードを頼りに、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▶用語集 P.182として安全である理由は、これらの方式を採用した無線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1人1人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、自分用の「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▶用語集 P.178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。ただし最近は、SIMカードを本人になりすまして再発行し、そのSIMの電話番号や情報を乗っ取る「SIMスワッピング詐欺」と呼ばれる攻撃により、無効化されてしまうことも指摘されています。フィッシング詐欺が起点となっていますので、注意しましょう。

2.9 自前の暗号化による盗聴対策

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://」▶用語集 P.177から始まるもののみ、メールでは「SSL/TLS」▶用語集 P.178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通信でサーバに接続するもののみを使用する方法です。

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、iOSでは、Appleのアプリ開発者向けガイドによるとスマホのOS▶用語集 P.177事業者が運営するアプリストアに登録するアプリには基本的にHTTPS通信を強制する「ATS」を有効にすることが求められています。

Androidでは Playストアのアプリダウンロード画面には通信の暗号化の有無が表示されます。盗聴や情報流出のトラブルがあるものは使用は控え、多くの人が使用しているアプリを使用した方が無難でしょう。

2.10 まとめて暗号化するVPN

こういった個別の面倒な対策で

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

上の表は、Android、iOS、macOS、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どう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。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。

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。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、macOS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。

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、利用者は皆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 個別のパスワード、クライアント証明書認証 ▶用語集 P.181（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。他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
○	WPA3パーソナル	AES/CNSA	鍵交換方式	WPA2における通信内容が解読されるリスクに対応するため、鍵交換方式を採用するほか、DDoSなどによる通信妨害等に対する機能の実装を義務付けた。なお2020年7月以降のルータでは対応が義務付けられている。WPA3エンタープライズでは、より強度の強い暗号をサポートしている。
○	WPA3エンタープライズ	AES/CNSA	鍵交換方式	

＊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。その他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。

自宅や会社のルータが感染状況が確認できる「am I infected?」

「am I infected?」https://amii.ynu.codes/

家庭や会社のルータやウェブカメラなどのIoT機器を狙ったサイバー攻撃が急増しており、今使用しているルータも感染しているかもしれません。

「am I infected?」は、横浜国立大学 情報・物理セキュリティ研究拠点が運営するマルウェア感染・脆弱性診断サービスで、ルータの感染状況を確認ができます。積極的に試して安全性を確認しましょう。

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）▶用語集P.178の個人利用です。

VPNとは元々は、地理的に離れた2点の事業者間をインターネットを利用しながら専用線で接続したかのように接続する技術です。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。

これを「事業所から事業所」ではなく、「個人のIT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1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。

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ので注意しましょう。VPNを利用したい場合は、そういった問題点を理解したうえで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であり、その先の通信の暗号化が行われない点は注意が必要です。

2.11 新規にスマホなど購入した場合に公衆無線 LANに関して行うこと

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。携帯電話キャリアと契約した場合、そのスマホには、キャリアから提供されているさまざまな方式の公衆無線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りますが、この設定を改めてすることです。

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。接続先が安全でない公衆無線LANのアクセスポイントであるとわかったら、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、切断した上で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。

2.12 公衆無線 LANが安全ではない場合の利用方法

なお、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、災害時に設置される「00000JAPAN」▶用語集P.176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。

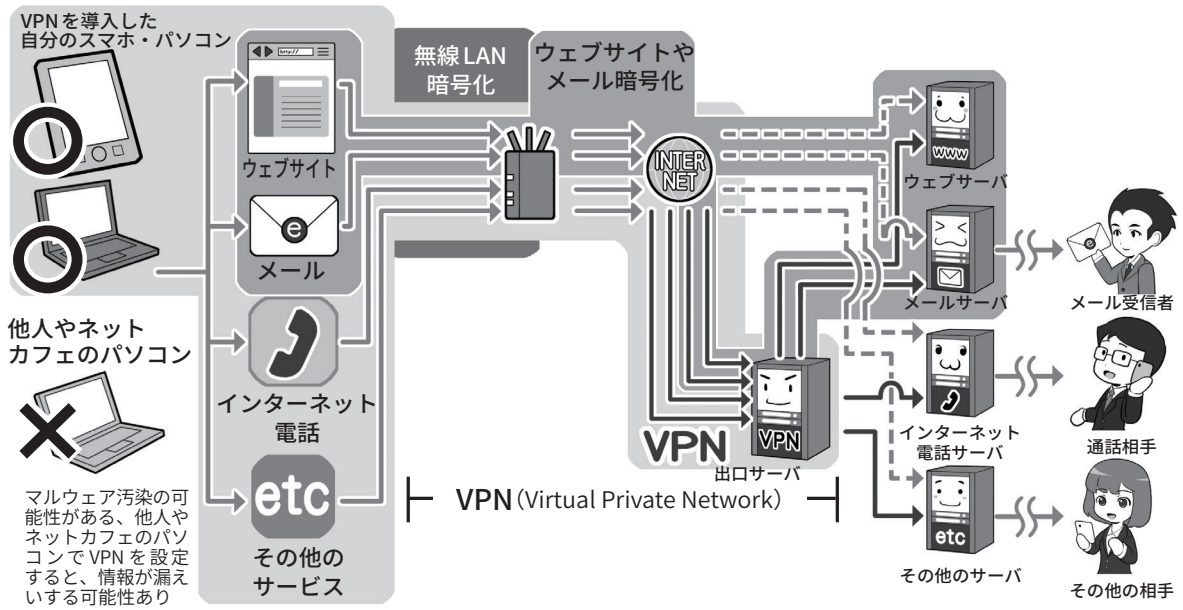
対策は、「無線LANの暗号化に頼らず、自前で通信を暗号化して盗聴対策をする」ことです。

例えば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」▶用語集P.185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。

しかし、災害時には、携帯電話回線への接続が難しい場合もあるでしょう。どうしても暗号化無しのネットワークを使わざるを得ないときは、流出して困るような重要情報を送信しない、最低限の使用に留めることを心掛けてください。

さまざま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



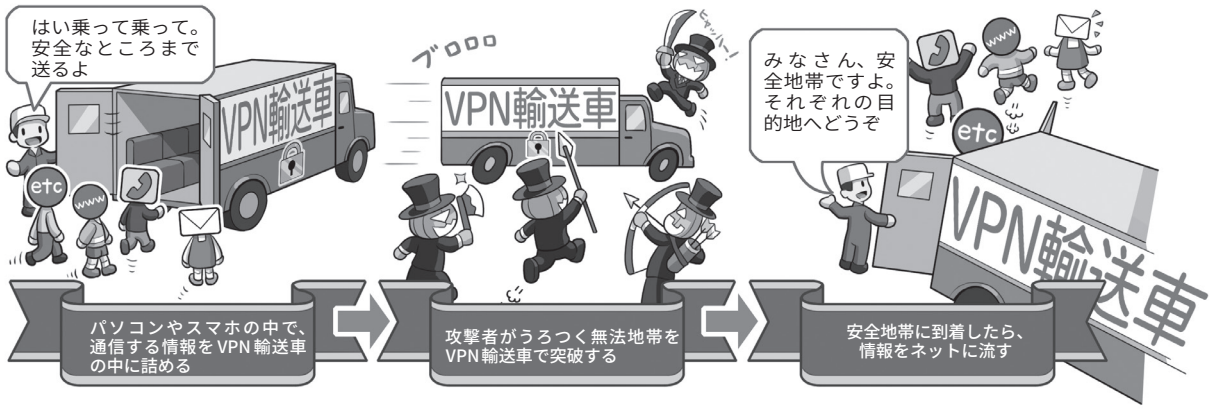
VPN を図で説明すると、上のように入り組んでよく分からなくなってしまうので、簡単な図を下に用意しました。くじけそうな方はまず下をご覧ください。

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、ウェブサイトやメールの暗号化、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、ウェブサイト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であり、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）でデータを輸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 安全なウェブサイトの利用を支える暗号化について学ぼう

3.1 無線LANの暗号化とVPNの守備範囲

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)▶用語集 P.178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▶用語集 P.180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には限界があり、したがって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、通信をする用途に限定して、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個別に暗号化するやり方があります。

3.2 すべての通信と、その一部であるウェブサイトとの通信

ウェブサイトを閲覧するための通信の暗号化において、無線LAN通信の暗号化とVPN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。そのほかに、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。

この多様な通信のことをテレビに例えるなら「テレビで視聴できるすべての電波放送(チャンネル)」と大きなくくりになり、ウェブサイトを閲覧する通信は、その中の1つのチャンネルにあたります。そして、通信にはさまざまなチャンネルが存在する、とすればイメージしやすいでしょうか。

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」▶用語集 P.188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とくになんの工夫をしなくても情報を盗むことができます。それのため「SSL(SecureSocketsLayer)/TLS(TransportLayerSecurity)」(以下SSL/TLS)という暗号化通信を用います。暗号化していないウェブサイト閲覧では、URLが「http://」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」の意味です。

3.3 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▶用語集P.180が表示されるか、問題がないという意味で、前ページ「3.1 無線LANの暗号化とVPNの守備範囲」の②や③の表示がなくなります。この場合「一応は」安全な状態と言えますが、最近はこの状態でも安全とは限らないケース見られます。

例えばSSL証明書▶用語集P.178の中には実在性確認をせず、簡単なオンライ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、審査の甘い認証局▶用語集P.185を使って、このような「SSL証明書」を取得して、例えば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手口がとられます。

3.4 より厳格な審査の「EV-SSL証明書」

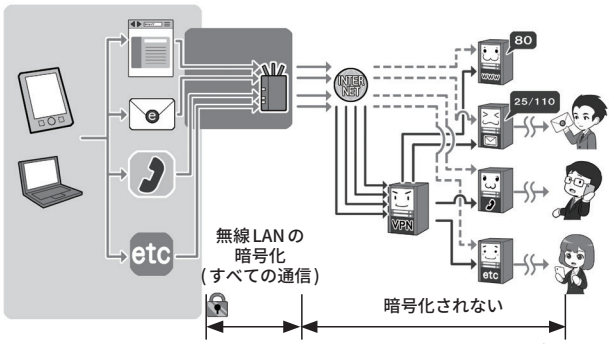
そういった問題に直面して、より審査を厳しくした「EV-SSL証明書」が登場しました。

「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

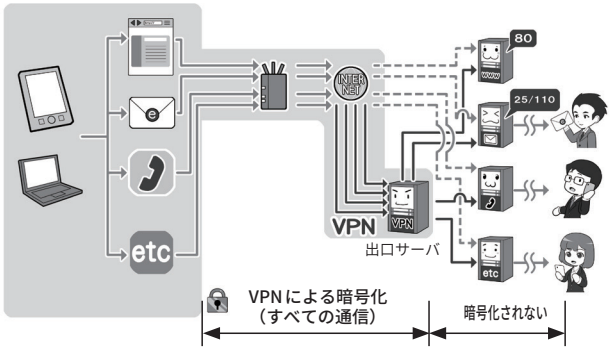
それぞれの暗号化の守備範囲

①無線LANの暗号化



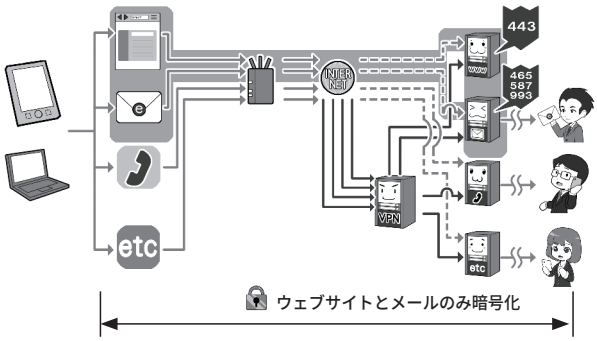
無線LANの暗号化は、利用者の機器から無線LANアクセスポイントまでのすべての通信を暗号化します。

②VPNによる暗号化



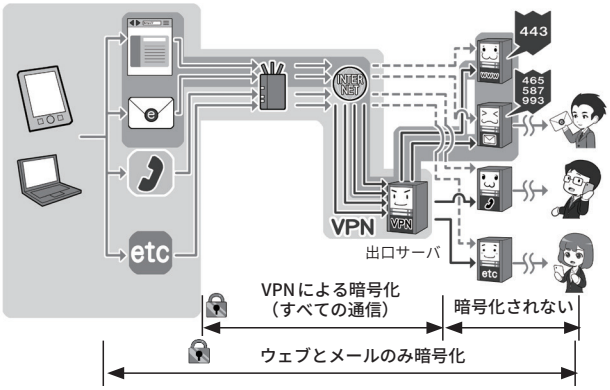
VPNは利用者の機器から、安全とされる「出口サーバ」までの区間で、すべての通信を暗号化します。

③ウェブサイトやメールの暗号化



ウェブサイト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、ウェブサイトとメールの通信だけを暗号化します。

④VPN＋ウェブメールの暗号化



ウェブサイト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。

です。

3.5 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▶用語集 P.180の通信が改ざんされないように「常時 SSL 化」▶用語集 P.182「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付けたりするようになったのです。

現在は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。

3.6 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

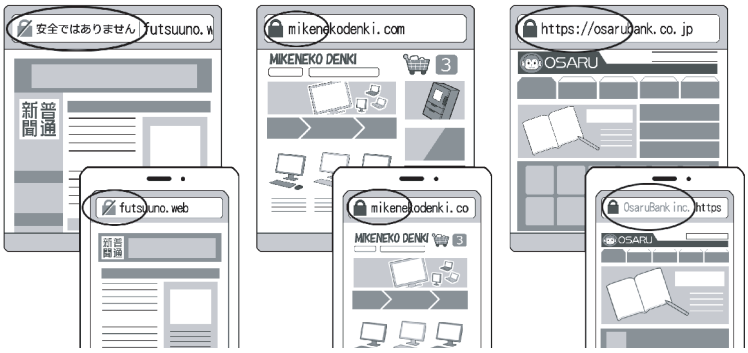
httpsの暗号化通信で情報を守る

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

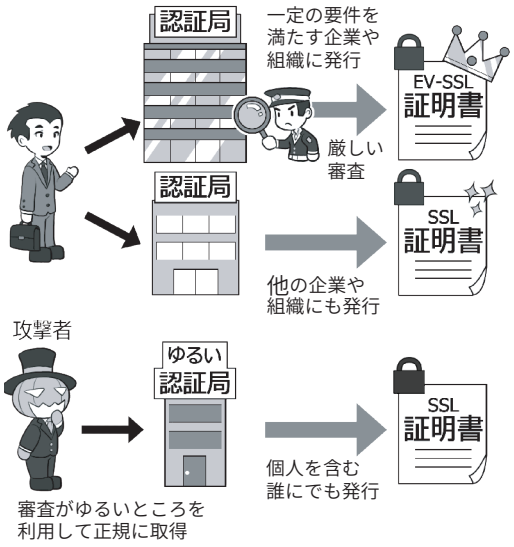
注意 △ SSL(暗号化あり)（https と表示される🔒マークが表示される）

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。とくに、お金関連のサイトは EV-SSL の方がより推奨されます。

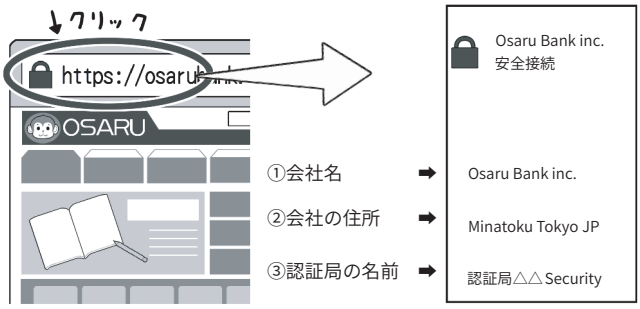
攻撃者が不正に取得した証明書に注意



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。

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▶用語集 P.183 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。

3.7 他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▶用語集 P.183 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）▶用語集 P.180**

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、通信面の他にも気を付けるべきポイントがあります。

例えば、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、これまで見たように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。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。

3.8 ウェブサイトを使ったサイバー攻撃に対応する

マルウェアの感染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▶用語集 P.187）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▶用語集 P.188、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▶用語集 P.188）もあります。

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▶用語集 P.180 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▶用語集 P.184 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▶用語集 P.182 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他、対処法はありません。

さらに、利用者を巧妙に騙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の存在を、自分が理解しなければ防げません。そのためにイントロダクション（P.25）で示した9か条の徹底が必要となります。

コラム.3 多要素認証すら破る「中間者攻撃」

二要素以上の多要素認証を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▶用語集 P.180 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。

偽サイトによる攻撃の手法は年々巧妙化しており、ウェブサイトの見た目などから見分けることは極めて難しいのが現実です。

例えば本物のサイトが、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が、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する方法があります。例えば「https://www.example.co.jp/foo/bar.html」のうち「example.co.jp」の部分を確認することです。ただ、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付きにくいのです。

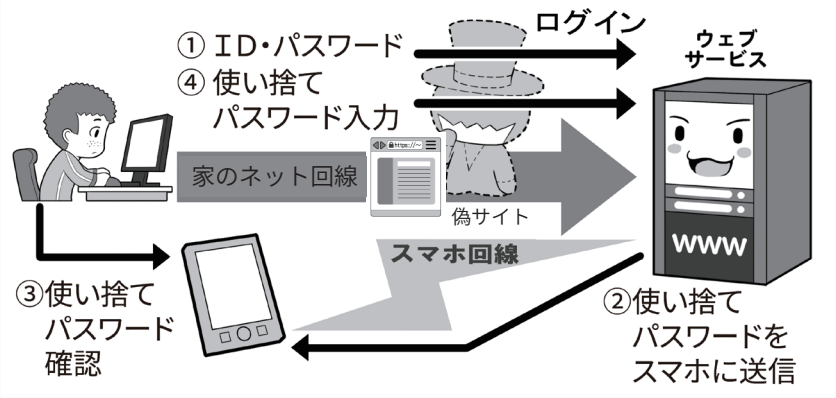
こういった状況を総合的に鑑みると、自分が利用するウェブサービスは、基本的にあらかじめブックマークしておいて、訪れる際も、詐欺に用いられやすい偽サイトへの誘導に使われるメールやメッセージのリンクは利用せず、直接ブックマークを開いてクリックして訪れるか、スマホの場合は公式のアプリを利用するのが安全でしょう。

もう1つ注意したいのは、野良Wi-Fi▶用語集 P.186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（P.115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、実際は偽サイトに誘導されてしまう場合があります。

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。

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。

ウェブサイトを使ったサイバー攻撃の例

①偽メールなどによる誘導　**②水飲み場攻撃による感染**

4 安全なメールの利用を支える暗号化について学ぼう

4.1 メールにおける暗号化

次は電子メールを安全に使う方法についてです。

「ウェブサイトを安全に利用する」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、メールの内容を盗み見されないためには、暗号化の区間が限定される無線LANの暗号化やVPNだけではなく、メールが送受信中、常に暗号化されていることが大切です。

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。

4.2 送信の暗号化と受信の暗号化

メールも、昔は送受信どちらも暗号化されていない平文で通信が行われていました。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▶用語集 P.188サービスで、暗号化によるメール送受信サービスが基本になっています。

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、最近ではとくに意識しなくても自動的にこの暗号化で通信を行うようになっているのです。

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。

とくに、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変えていない場合、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。

メールアカウントをたくさん持っている人は、一度メールアカウントの棚卸(たなおろし)をし、設定を見て暗号化されていないアカウントがあれば、暗号化している方式に切り替え、暗号化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、そもそも安全ではないと考え、暗号化方式が提供されている安全なメールサービスに乗り換えるようにしましょう。

4.3 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な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、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、内容は読まれてしまう余地はあります。

それは現代でも外国に郵便を送ると、国や地域によっては検閲で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▶用語集 P.185が保障されるか否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とりするように、メール送受信を暗号化したサービスの中だけでやりとりする方法もあります。

4.4 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」▶用語集 P.178 という方法と「PGP」▶用語集 P.177 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、もともと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▶用語集 P.181 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。

とくに S/MIME を使う場合は、お金を払い認証局が発行する証明書を入手し、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、仮にメールの本文を改ざんされても、受信者側で改ざんされていないか調べ

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通信（SSL/TLS）利用することになっているか？

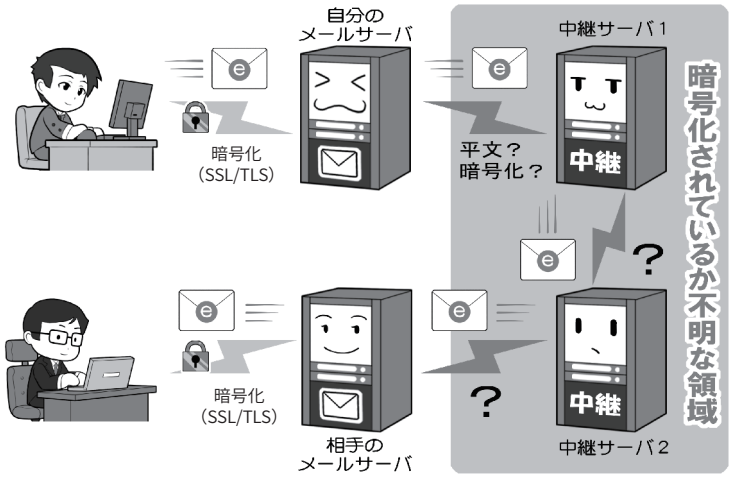
メールソフトの例

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。

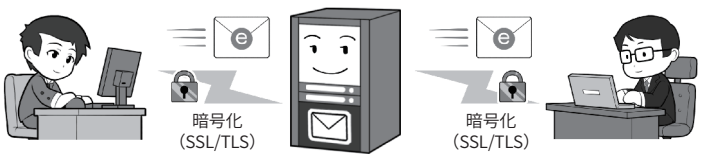
「受信ポート587や993の使用」、「送信ポート465の使用」、「パラメータとしてSSL使用がオン」などになっているかがチェックポイントです。これらは暗号化通信が設定されている目印です。

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 1 つの方法としては、暗号化通信を採用した 1 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とりするのと同じ概念です。

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。これを実現する技術を「デジタル署名」▶用語集P.185と呼びます。

上記のとおりS/MIMEは大変優れた機能ですが、事前の準備に手間がかかり、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。

なお、サービス側でメール送信者の成りすましを防ぐ技術として、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。

これらを採用したサービスがあれば、積極的に利用を検討してもよいでしょう。それが安全な技術の普及への一助になります。

4.5 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▶用語集P.187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し注意喚起しています。

この場合、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うかつに開くと「ゼロデイ攻撃」▶用語集P.184などを受け、不

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。

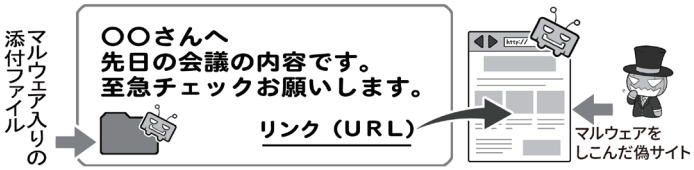
一般的には「SSL証明書」や「EV-SSL証明書」を持ち、暗号化通信を示す鍵マークがついていることで、暗号化されているかどうか、信頼性があるかどうかなどがわかります。

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。

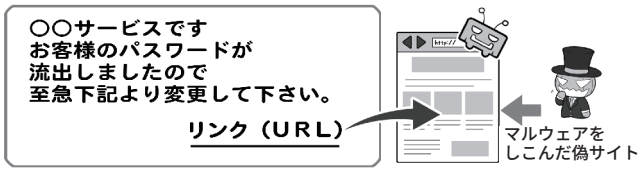
怪しいメールとはなにか

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。名前を語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。

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ばらまき型の「スパムメール」▶用語集 P.183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こともあり、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、偽装広告へのリンクをクリックさせたりする洗練された手法なのです。

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、緊急に文中のリンクや添付ファイルを開くことを要求するメールなどは、かなり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付けてください。

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・ウェブ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。

4.6 マルウェア入りの添付ファイルに気を付ける

「怪しいメール」の１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付けられます。

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。

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」▶用語集 P.181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、拡張子は「.exe」▶用語集 P.176となり、exe と表示されれば「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、文章ファイルに見える「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。

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。

なお通常のメールのやりとりで、従来ファイルを送付する際に、送付ファイルをパスワード付き ZIP ファイル化して添付ファイルとして送信

し、別メールで、パスワードを送信するPPAP（(Password付きZIPファイルを送ります、Passwordを送ります、Angoka(暗号化)Protocol(プロトコル))の略号))と呼ばれる手法が多く用いられてきました。しかし、ファイルを添付するメールと、パスワードを送付するメールは、多くの場合に同じ宛先に別メールで送ることから、盗聴防止や誤送信防止などの関係では「暗号化」の意義は小さいほか、マルウェア検知の仕組みを講じた場合でも、ファイルの内容を確認できないことで、Emotetなどのマルウェアを検知することができず、却ってリスクを高めているという指摘があり、実際に被害も発生しています。

したがって、PPAPによるファイル送付は基本的には行わないようにし、他の方法を用いてファイルなどを共有できるようにすることが必要です。

なお、例えば、パスワードは都度送付するのではなく、事前に合意したものを使用するなどの方法も考えられますが、この場合でもマルウェアの検知が難しくなることには変わりありません。

対応策としては、例えば、安全性の高いファイル送付システムのサービスを利用する、ウェブ上でのストレージサービスなど、ファイル共有サービスを用いる等が想定されます。

4.7 ウェブサービスなどからのメールアドレスの流出

「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。

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▶用語集P.184)で名簿として売買されることもあります。

では流出が判明した場合、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。

4.8 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、親しい人とやりと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、複数の仮想メールアドレスを作れ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」▶用語集P.185「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。

1つのサービスからの流出によって他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ば、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あれば、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(次ページ右下図参照)。

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同様に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、まずは自分から流出させないようにしましょう。

4.9 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とり」にもあてはまります。

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1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、さまざまなシステムや機器がつながりあって情報をやりとりする、「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。

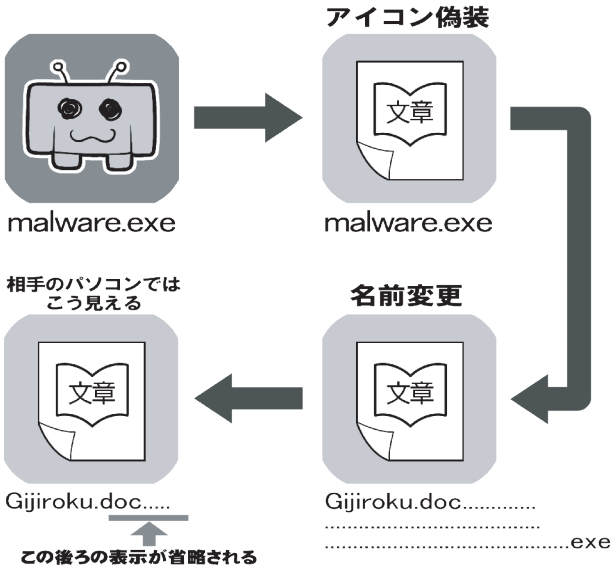
メールは特定の企業サービスとは紐付かないインターネットの仕様なので、さまざまなメールソフトを使い、どのメールサーバに接続しても基本的には利用可能なのです。

1社によって提供され、栄枯盛衰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さまざまなOSやメールソフトを乗り継いでも、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。

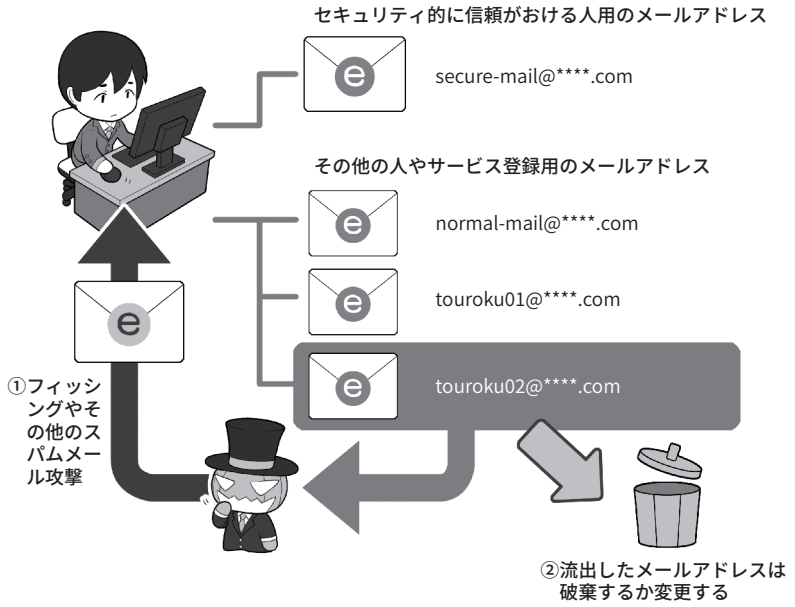
SNSや各種通信サービスなどはサービス終了時にデータのエクスポート(出力)の対応をすることもありますが、それらは保存されるデータであって、データが生きていた環境はサービス終了とともに終わってしまうわけです。その分、メールにはない、さまざまな華やかな機能を楽しむこともできます。

SNSとメール、どちらがよ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。



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 安全なデータファイルの利用を支える暗号化について学ぼう

もう1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感染で流出したり、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。

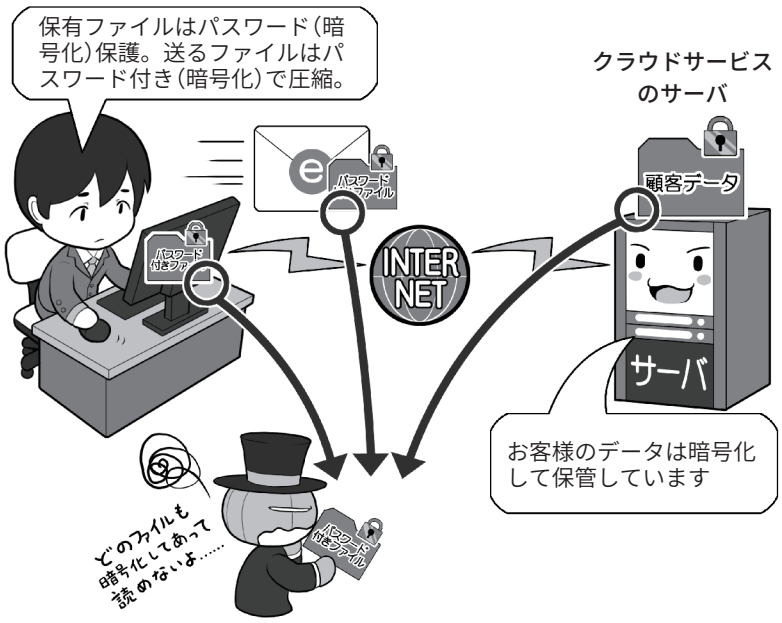
ただ、ファイルの暗号化は、攻撃者に盗まれると高速なコンピュータを使って執拗に解読を試みられ続ける可能性があります。したがって「暗号キー」の基準にしたがって、長く複雑なものを設定しなければなりません。

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の付いた外付け記憶装置やUSBメモリの利用が想定されます。

外付け記憶装置やUSBメモリは、最近では大容量のデータの持ち出しが可能となり、漏えい時の被害が大きくなります。そのため、高速に暗号処理が可能でさまざまな攻撃に対策された暗号化チップ▶用語集 P.180が内蔵された記憶装置を選択しましょう。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。

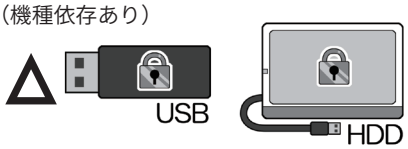
USBメモリの場合、汎用性と安全性を両立した、ハードウェアキーでPINコード相当の認証をするタイプもあります。これらは専用の認証用ソフトウェアを必要としないので、利用するOSの依存度が少ないのと、ハードウェアキーの入力を「PINコー

データの暗号化は保険

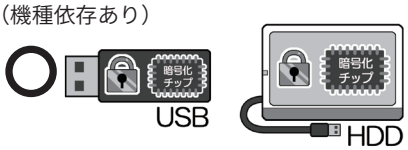


データを持ち運ぶときは必ず暗号化メディアを使う

ソフトウェア暗号化＋パスワード入力ソフト（機種依存あり）



ハードウェア暗号化＋パスワード入力ソフト（機種依存あり）



ハードウェア暗号化＋指紋認証 or ハードウェアキー（機種異存が少ない）

＋「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。

ド」方式と同じにすることで、入力を間違えると「ロック」や「データ消去」の保護機能があります。内部では「暗号キー」として十分に長く複雑なものが自動で生成され、この「暗号キー」の利用にのみ「PIN コード」の入力を求めることで利便性と安全性を両立しています。

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。

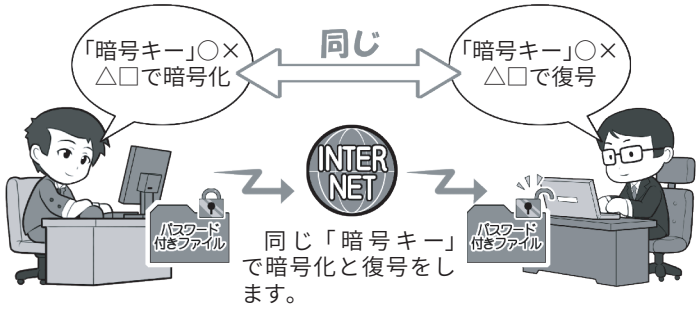
「暗号キー」は英大文字小文字＋数字＋記号で、完全にランダムな 形で、できるだけ桁数を増やすことが推奨されます。

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付けなければなりません。特に本章 4.6(P.127) でも述べたように「PPAP」は避けることが重要です。どうしても暗号化したメールを送付しなければならない場合には、「暗号キー」はメールでは送信せず、事前に対面や、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。

さらに、「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、こういったシーンでは目にしません。

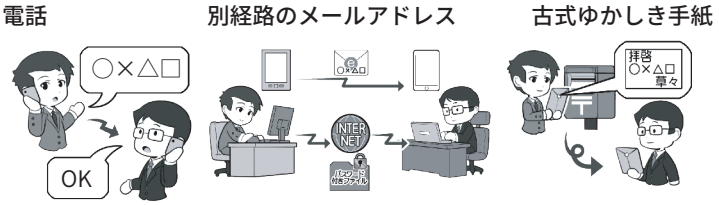
ただ、この方式は、本章 4.4(P.124) で紹介した「S/MIME」や「PGP」や、同じように目にすることはありませんが、無線 LAN 通信の暗号化など、見ていないところでファイルも暗号化しています。

「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



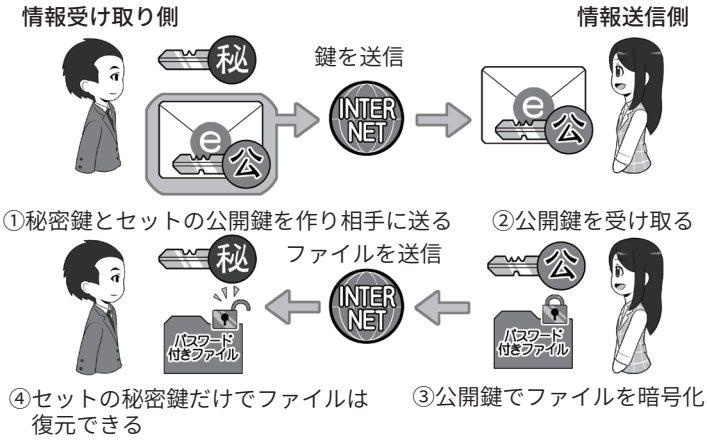
直接会ったときに「暗号キー」を渡したり、電話で直接伝えたりします。

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１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.4 「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、無料提供されているわけです。

その方法の1つは広告による収益モデルです。広告主がウェブサイト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、趣味や行動などの情報を収集し、一見匿名の情報の形にして、これを広告おもに提供、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、利用者が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▶用語集P.188を行う型もあります。

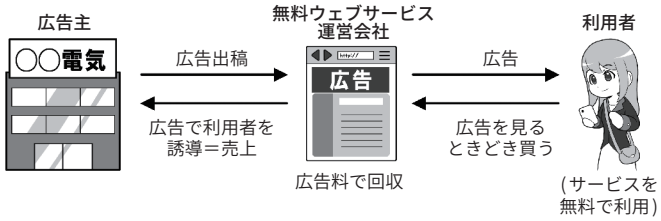
そして最後に最も気を付けたいのが善意の無料サービスです。誰かがウェブサービスやアプリなどを開発し無料で提供するのですが、明示的ではなくても「責任は一切取りませんよ」という状態のものです。

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、

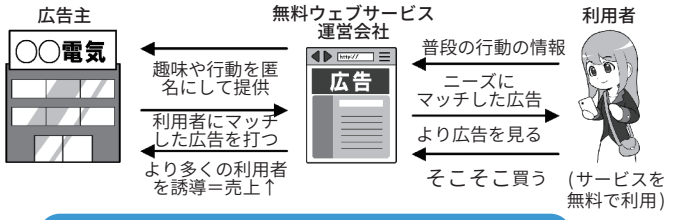
試食コーナーのサービスコストの例

無料ウェブサービスの例

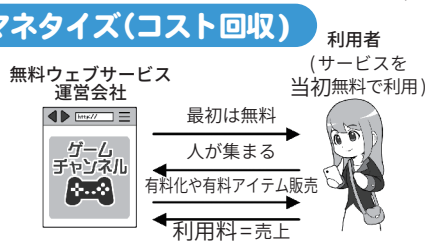
①無差別広告で運営



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(コスト回収)



④セキュリティ意識の低い善意の無料サービス

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」といった方がよいでしょう。

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。

そして今回も問題なのは「善意の無料サービス（ただし責任能力なし）」です。

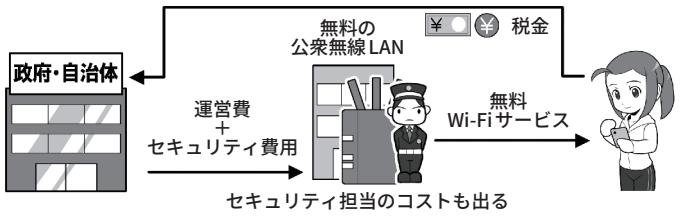
小さなお店などで無線 LAN が提供されている場合、それは自宅用や仕事用のものを無料開放しているだけかもしれません。そして無料で使っている以上利用者とは契約関係もなく、利用する側は安全性を求める権利もないわけです。

そして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が忍び込み罠を張っているかどうかなど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、セキュリティ意識の低い、無料の公衆無線 LAN は推奨されない」というわけです。公衆無線 LAN を使うに際しては、総務省から提供されている「公衆 Wi-Fi 利用者向け 簡易マニュアル」が参考になります。

無料という言葉には注意が必要です。運営されている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。

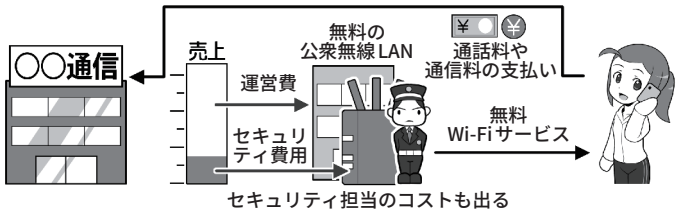
無料の公衆無線 LAN サービスの例

①一見無料だが税金などでまかなっている間接的に有料



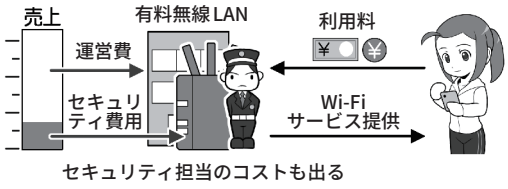
トラブルがあると議会などで取りあげられ問題となることもあります。責任能力もあります。

②企業が収入の中から払っているから（追加料金）無料



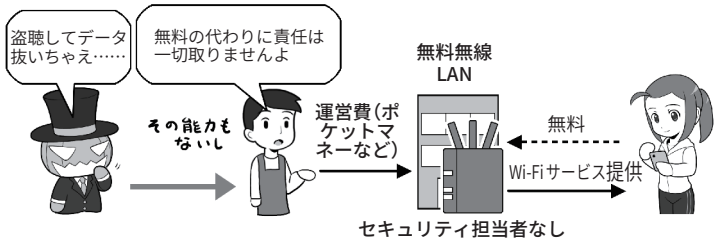
トラブルが起きれば責任問題となり、本業にも影響が出ます。責任能力もあります。

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セキュリティ意識の低い善意の無料サービス



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、実質的に責任は取ってもらえません（その能力もありません）。

コラム.5 クラウドストレージサービスからの情報流出。原因は？

クラウドストレージサービスとは、「従来手元で保存していたデータなどを、インターネット上に存在しているサーバに保存し、ネットにつながったどの機器からでも利用できる」サービスです。ネットワークの図の上にインターネットを描く場合、雲(英語でクラウド：cloud)を描くことが一般的であったことから、インターネット上で提供されるサービスをクラウドサービス(略してクラウド)と呼ぶようになりました。

クラウドは大変便利ですが、きちんと利用目的とセキュリティを固めて利用しなければ、攻撃者の格好の的になると、理解してから利用しましょう。

とくに、スマホとクラウドは切っても切り離せないものとなっています。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サーバ▶用語集 P.181にバックアップされていることもあります。スマホからでもウェブブラウザからでもアクセスできるメールサービスもクラウドサービスです。

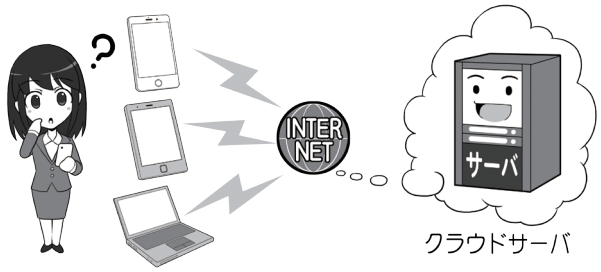
まず、クラウドストレージ上に他人に見せたくないデータがあれば、公開設定や共有設定などのアクセス権限に気を付けましょう。

誰でもアクセスできる設定になっている場合、自分の知らないうちにデータを他人に見られてしまうかもしれません。

また、他人にIDとパスワードを知られてしまうと、自分になりすまして不正アクセスされてしまいます。有名人が狙われるケースや個人がストーカーなどに狙われるケースの原因の多くは不正アクセスであり、こういった不正アクセスによる情報流出を起こさないためには、まずパスワードを複数のサービスで使い回ししないこと。そして、推測されるほど簡単なものにしないこと。セキュリティの強化を目的として多要素認証などや、不正なアクセスがあった場合通知される機能が提供されていれば可能な限り利用すること。そして本当に流出して困る情報は、クラウドサーバにアップロードするかどうか十分吟味することです。

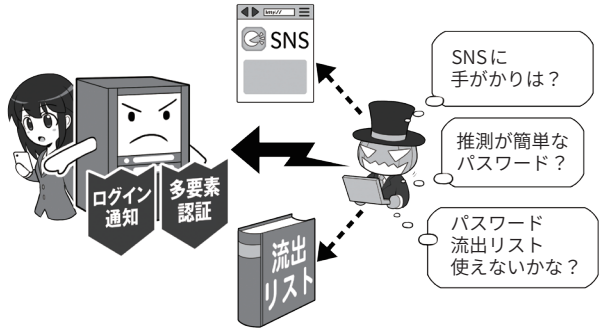
クラウドを利用するに際しては、上述のように適切な設定を行うことが重要です。またクラウドの設定に関する権限や設定のミスを突いて、外部からの攻撃を受けることになってしまい、情報漏えいが生じる事例などもあります。クラウドサービスの中には、例えば情報の非公開の決定や他のサービス連携の選択を行うための管理権限を、利用者に与えていないものもあります。この場合には、予期しない形で情報の漏えいが生じる危険性を伴うため、サービス利用前に十分確認しましょう。なお、総務省では情報の流失のおそれに至る事案の発生を防止する観点から、クラウド設定についてわかりやすく解説した「クラウドの設定ミス対策ガイドブック」を策定しているので、こちらも活用しましょう。

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、全く意識せずにクラウドサーバ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付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、さまざまな攻撃を試みます。「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、パスワード設定の基本を守るとともに、サービス間で使い回しをせず、多要素認証の設定や不正なログインがあった場合に通知を受け取れる設定を活用しましょう。