特集2

消費者が知っておきたい情報セキュリティ対策

佐條 研 Sajo Ken
一般社団法人JPCERTコーディネーションセンター レスポンスグループ マルウェアアナリスト
ばらまきメールや標的型攻撃の脅威動向分析、インシデント対応業務に従事するほか、啓発活動なども行っている

サイバー攻撃を知る

JPCERTコーディネーションセンターはサイバーセキュリティ上の問題・事件(以下、インシデント)の発見と対処、被害の抑止に向けた活動を行っており、国内外のさまざまな個人・組織からインシデントの報告を受けています。当センターに寄せられた過去5年間のインシデントの報告の推移を図1に示します。図から分かるように、年々増加しており、消費者がサイバー攻撃に遭遇するケースが増えているといえます。

報告を受けたインシデントをカテゴリー別に分類したものが図2になります。全体の報告のうち、3分の2はフィッシング攻撃に関する報告であり、標的となっているのは個人消費者です。それ以外のスキャン*1やウェブサイト改ざん*2なども個人消費者が標的となっているものが多いです。

高度な標的型攻撃と呼ばれるものを除くと、一般的にサイバー攻撃というのは、金銭やそれに代わるものを窃取することを目的としています。その手段として被害者を騙(だま)すことで攻撃を成功させようとします。そのため、サイバーセキュリティ対策として必要なことは、まずはど

図1 年間報告件数の推移(年度比較)

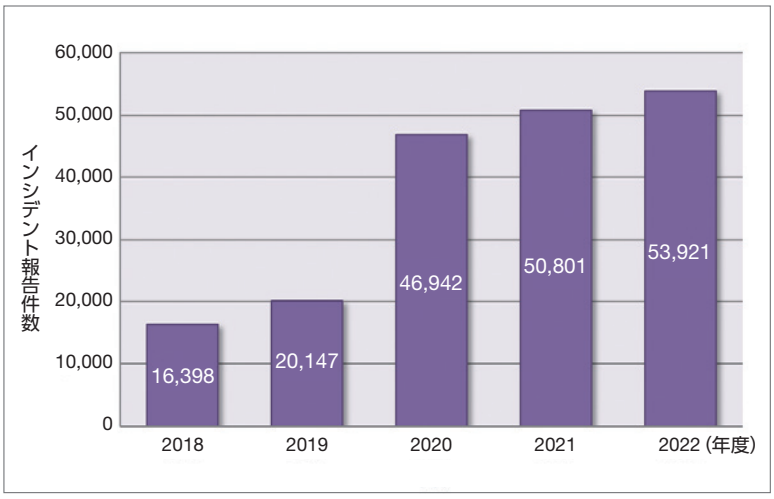
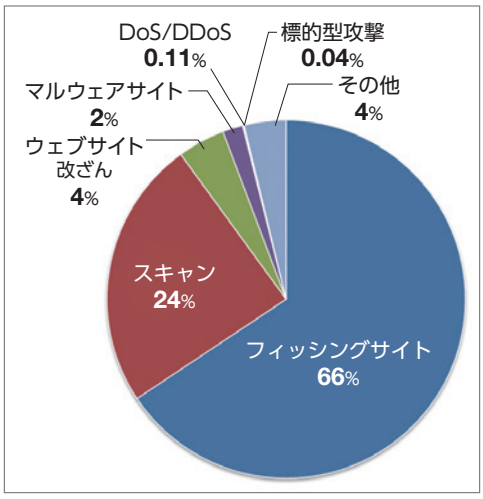


図2 報告を受けたインシデントのカテゴリー別割合(2023年1月～3月)



出典:一般社団法人JPCERTコーディネーションセンター「JPCERT/CC インシデント報告対応レポート 2023年1月1日～2023年3月31日(第3版)」(2023年4月18日) https://www.jpcert.or.jp/pr/2023/IR_Report2022Q4.pdf

*1 サーバーやパソコンなどの攻撃対象となるシステムの存在確認や、システムに不正に侵入するための弱点(セキュリティホールなど)を発見するために、攻撃者によって行われるアクセス(システムへの影響がないもの)を指す。また、マルウェアなどによる感染活動も含まれる

*2 攻撃者もしくはマルウェアによって、ウェブサイトのコンテンツが書き換えられた(管理者が意図したものではないスクリプトの埋め込みを含む)サイトを指す

のような攻撃があるかを知り、注意すべき点を知ることです。昨今のサイバー攻撃の傾向や事例(**特集1**参照)について知り、どのような時にどのような点について注意を払って行動するべきかを知ることが重要です。

パスワードの管理

サイバー攻撃で最も狙われる対象の1つはアカウントとパスワードの「認証情報」です。パスワードは文字数や使う文字によって安全さが異なります。当センターでは安全なパスワードの条件として次の条件を満たすものを推奨しています。

安全なパスワードの条件

- パスワードの文字列は、長めにする(12文字以上を推奨)
- 大小英字だけでなく、さまざまな文字種(数字、記号)を組み合わせる
- 推測されやすい単語、生年月日、数字、キーボードの配列順などの単純な文字の並びやログインIDは避ける
- ほかのサービスで使用しているパスワードは使用しない

しかし、複雑で安全なパスワードをサービスごとに作成し管理するのは利用するサービスが少なければ可能ですが、多くなると管理するのは困難になります。管理が難しい場合は、信頼性のあるパスワード管理ツールを使用しましょう。

多くのパスワード管理ツールでは、インターネットサービスごとにアカウントIDとパスワードを一度登録しておけば、利用する際にツールから呼び出して自動入力することができます。したがって、利用者はツールを起動するためのパスワード1つを覚えてさえいればよく、サービスごとに異なる複雑なパスワードをすべて覚えておく必要はありません。サービスごとの複雑で安全なパスワードもパスワード管理ツールが自動的に作成することも可能です。多くのパスワード管理ツールはパソコンとスマートフォンどちらでも一貫して利用することが可能となっています。

パスワード管理ツールを使うことのメリットは、複雑なパスワードを覚えておくのを任せることができるという点だけではありません。そのパスワードを入力するべきサイトをセットで覚えているため、ほかのサイトに誤入力することがないという点です。例えば、フィッシングサイトを訪れてしまってパスワードを入力しようとしても、正規のサイトではないためパスワード管理ツールが入力を行いません。そのことを理解していれば、フィッシングサイトであることに気がつきパスワードを入力してしまうこともなくなるでしょう。

さらに、より強固なセキュリティ対策として携帯電話へのSMSやトークン[*3]、スマートフォンアプリなどを使用したワンタイムパスワードを使った2段階認証があります。アカウントIDとパスワードによる認証に加えて、ログイン時に一定時間だけ有効なパスワードを使用してログインを行うしくみです。もしパスワードとワンタイムパスワードが盗まれてしまった場合でも、ワンタイムパスワードは毎回変化するため、利用者の手元で確認する最新のワンタイムパスワードがない限り、不正なアクセスを防ぐことができます。パスワード管理ツールと合わせて使うとより効果的です。

ウイルス対策ソフトの利用

ツールでできるセキュリティ対策はほかにも

＊3 ワンタイムパスワードを生成する機械やソフトウェアのこと。非接触型やBluetooth型、PCカード型、USB型などがある

あります。まず優先すべきことはパソコンへウイルス対策ソフト、スマートフォンへウイルス対策アプリなどのツールを導入しておくことです。

ウイルス対策ソフトは、パソコンがコンピューターウイルスに感染した時に見つけ出すことができます。初めからインストールされているウイルス対策ソフトでもある程度はブロックしてくれますが、製品によってはインターネットでアクセスするウェブサイトが不審なものかどうかを判定しブロックしてくれる製品もあります。例えば、コンピューターウイルスに感染するおそれのあるウェブサイトやフィッシングサイト、偽ショッピングサイトなどを検知してブロックしてくれます。こういった製品を選んで導入すれば、ウイルス対策ソフト1つでコンピューターウイルスの被害と悪意あるウェブサイトの被害の双方からデバイスを守ることができますので検討してください。

なお、ウイルス対策ソフトが新しい脅威を検知するためには、定期的にセキュリティサービス提供元へ通信し、脅威情報をアップデートする必要があります。ウイルス対策ソフトを導入すると定期的に自動で通信する設定になっているため、そのままの設定にしていれば問題はありませんが、有償のウイルス対策ソフトであれば1年ごとなど定期的にライセンスを購入し更新する必要があります。ライセンスの切れたウイルス対策ソフトは導入していても効果はほぼありませんので、注意してください。

ただし、ウイルス対策ソフトといえども、ウイルスの発見も危険なウェブサイトのブロックも完璧に行えるものではないことには注意が必要です。ウイルス対策ソフトが警告を出さなかったからといって必ずしも安全といえるわけではありませんので、不審なファイル、不審なサイトだと思われたときには、より安全な対応となるように不審なものは触れないようにしてください。

ソフトウェアの定期更新

定期的に更新が必要なものはウイルス対策ソフトだけではありません。すべてのソフトウェア、アプリは新しいバージョンが出たら更新する必要があります。なぜ更新が必要なのでしょうか？

ソフトウェアのバージョンアップには主に2つの内容が含まれています。1つは機能の追加、もう1つはソフトウェアの不具合の修正です。後者の不具合の修正には、ソフトウェアにできてしまったセキュリティ上の“穴”を修正するものが含まれます。ソフトウェアを作る際にはセキュリティに考慮して作成されますが、それでも意図しない挙動が発生してしまうことがあります。それは脆弱性（ぜいじゃく）と呼ばれるセキュリティ上の“穴”（セキュリティホール）となり、これがサイバー攻撃に悪用されることがあります。こういった脆弱性を防ぐためにソフトウェアに新しいバージョンが出たらバージョンアップする必要があります。製品によってはセキュリティの適用をまとめたものをバージョンアップとしてではなく「パッチ」と呼んで提供しているケースもあります。その場合は「パッチの適用」と呼ばれます。

バージョンアップが必要なソフトウェアの中で一番重要なのは、パソコンやスマートフォンの基本のソフトウェアであるOSです。パソコンであればWindows、Mac OS、スマートフォンであればAndroid、iOSです。これらは基本のソフトであるために最もセキュリティ上の穴になりやすく、OSの提供元が定期的にバージョンアップの提供を行っています。例えばWindowsであれば毎月OSのアップデートが提供されていますので、提供されたらアップデートを適用しましょう。スマートフォンの場合はOSのアップデートまでの期間が長い傾向がありますが、代わりにアプリの更新が頻繁に行われています。

設定可能であれば自動で更新されるように設定しましょう。ただし、OSにはサポート期間という概念があります。古い製品を使い続けているとサポート期間が終了して、バージョンアップやセキュリティパッチの提供がなくなってしまいます。そういった製品を使い続けることはセキュリティが担保できなくなるため、よくありません。古いパソコンやスマートフォンは性能も低くなりますので、OSを更新する意味でもパソコンであれば3～5年、スマートフォンであれば2～4年に1度を目安に買い換えるのがよいでしょう。

バージョンアップが必要なのはOSだけではありません。特にサイバー攻撃で狙われることが多いのは、ほかにブラウザー、オフィスソフト、メールソフト等です。また家庭にある機器で狙われるものにルーターがあります。ルーターは基本的には自動で更新されますので、標準のパスワードを変更したうえで、定期的に更新される設定になっていることを確認してください。

ウェブサイトのセキュリティ対策

ソフトウェアの定期的な更新が必要なのは家庭内の機器だけではありません。人によってはサーバーを借りるなどして、ウェブサイトを持っていることもあるのではないでしょうか。その場合にはウェブサイトを構成するソフトウェアもまた同様に定期的な更新が必要になります。ウェブサイトは基本的には誰からも見られるようインターネットに公開されているため、利用者と同じように攻撃者もアクセスができます。そのため、セキュリティ対策の“穴”があればすぐに狙われてしまいます。

サーバーを借りている場合にはどのようなOSやソフトウェアが使われているかを把握しておく必要があります。特にWordPressなどのコンテンツ管理ソフトを使っている場合には、プラグインも含めて把握したうえで、パソコンと同様にOSとソフトウェア、プラグインのアップデートを定期的に行う必要があります。対して、クラウドサービスを利用してウェブサイトを公開している場合にはサービス提供側がソフトウェアを一括して管理していますので、アップデートを個人が管理する必要はなくなります。ウェブサイトのソフトウェアの管理が難しい場合にはクラウドサービスを使うことも検討してください。

どちらの場合でも、管理者アカウントのパスワードは、複雑で安全なものにする必要があります。ウェブサイトは公開するという意識とともに管理するという意識も必要になります。管理できない場合にはウェブサイトをクローズする、あるいは管理できる人に依頼する、といったことも考える必要があります。

サイバー攻撃は誰もが狙われる

昨今のサイバー攻撃は企業や個人、業種業界を問わず標的とします。その中でも特に狙われるのは、セキュリティ対策が不足している所です。セキュリティ対策が不足している人からアカウント情報を窃取し、セキュリティ対策が不足しているパソコンやアプリは踏み台として他所への攻撃に悪用されたり、自組織への侵入経路として使われたりします。

インターネットを利用するうえでは誰もがセキュリティ対策をする必要があります。セキュリティの脅威を知らないということは、詐欺師に騙される可能性が高くなるのと同じであり、セキュリティ対策を行わないということは、家に鍵をかけずに留守にするのと同じようなものです。本記事をきっかけとして、取り組めそうなものからセキュリティ対策を行っていただければと思います。