サイバー犯罪対策の基本は「今」を知ること

●いきなり脅迫状を表示する「WannaCry」の脅威

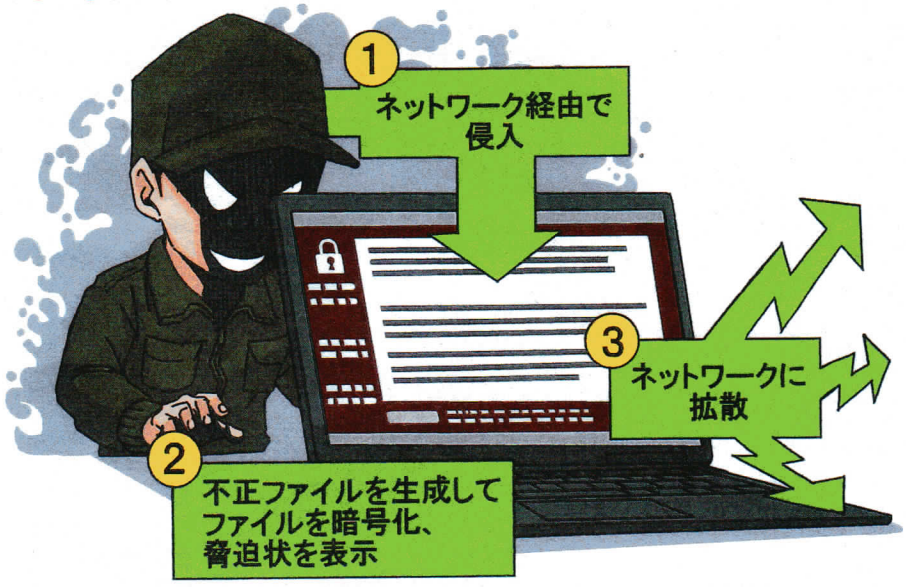


図1　2017年5月に世間を騒がせた「WannaCry」。更新していないWindowsの脆弱性を突いて入り込み、不正ファイルを生成してファイルを暗号化。身代金要求の脅迫状を表示するランサムウエアだ

●これまでの常識が通じないサイバー犯罪の巧妙化

3年前の常識	巧妙化する攻撃
外国語のメールは開かない	日本語の巧妙なフィッシングメール
怪しいサイトは見ない	一般的なWebサイトも危ない
セキュリティソフトを入れている	非対応の最新ウイルスが次々と出現
SNSはやっていない	家族や知人から情報が漏洩する危険性
ソフトは更新している	更新する直前のゼロデイ危機
違法なファイル交換をしていない	通常のダウンロードでもウイルス感染
パソコンはしっかり保護している	スマホやIoT機器からも感染

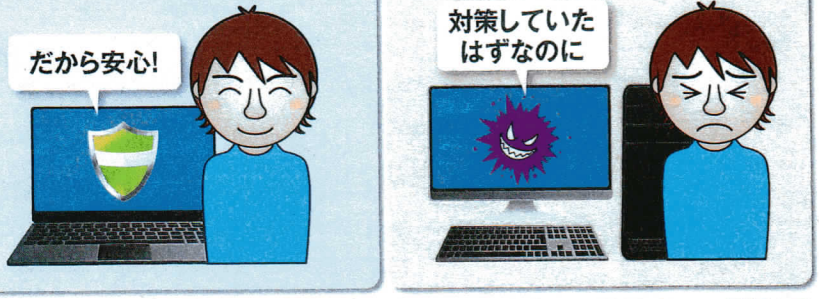


図2　「怪しいメールは開かない」といった3年前の常識だけでは通じない。最新の手口を知らないと、サイバー犯罪の被害者や加害者になりかねない

イラスト：ヨーダヒデキ

ある日突然、パソコンの画面に身代金を要求する脅迫状が表示されたら、驚かない人はいないだろう。2017年5月、世界中で猛威を振るった「WannaCry（ワナクライ）」は、データファイルを暗号化し、身代金を要求する「ランサムウエア」だ（図1）。ネットワーク上で拡散を続け、日本でも大手企業のネットワークが被害を受けたことは記憶に新しい。

必要なのは最新の防御策

ネットワークに接続する環境が当たり前になった今、「怪しげなメールは開かない」といった常識は多くの人が持っているだろう。しかし、そんな対策だけでは、現在のサイバー攻撃には対抗できない。

WannaCryが標的としたのは、古いWindowsの脆弱性だ。適切に更新していれば防げたはずの被害だが、さまざまな理由で残っている未更新のパソコンのせいで、被害が世界中に広がってしまった。

隙を突いて入り込んでくる攻撃者から身を守るには、現状を正確に理解し、新たな対策を立てる必要がある（図2）。図3にまとめたのは、現在起こっているサイバー犯罪から考えられる最小限の対策だ。この7カ条を実践していれば、サイバー犯罪に出合う確率を低減させることができるだろう。

サイバー犯罪対策として、まず見直したいのが、Windowsのサインインだ。パスワードの入力を省略す

用語解説

PIN▼
personal identification numberの略で暗証番号のこと。Windows 10では4桁以上の数字をPINコードとしてパスワードの代わりに利用できる。

Creators Update▼
2017年4月に公開されたWindows 10の最新バージョンのこと。バージョン番号は「1703」。Windows Update経由で更新できる。

るのは玄関の鍵を外すようなもの。起動時はもちろんのこと、スリープからの復帰時にもサインインは必要だ。破られにくいパスワードを設定して、侵入者を防ごう（図4）。大事なデータを守りたいなら、生体認証機器の導入も考えたい。

最小4桁の数字でサインインできるPINコードはパソコン単体にひも付けられるため、漏れたとしてもそのパソコンがなければ使えないという利点がある。家庭内で使うデスクトップパソコンなど、使用環境によってはPINコードを使うのもよいだろう。

最新版でセキュリティ強化

Windowsは世界で最も使われているパソコン向けOSだ。それだけに攻撃者のターゲットとなりやすい。そこでマイクロソフトは「Windowsファイアウォール」や「Windows Defender」など、サイバー攻撃に対応する機能を進化させてきた。

Windows 10の最新更新プログラムである「Creators Update」では、不正アプリへの対策として、Windowsストア以外からのアプリのインストールを警告する機能が追加された（図5）。また、「Windows Defender」が「Windows Defenderセキュリティセンター」の一部となり、セキュリティ関連の機能を一括して設定できるなど、強化が図られている（図6）。サイバー犯罪に対抗するには、こうした最新版へのアップデートが欠かせない。

この特集では、サイバー犯罪の主な原因となっているWebサイトとメールを中心に、対策を考えていこう。

●最新セキュリティ対策基本7カ条

1. ソフトウエアは最新版に更新
2. メールからWebサイトにアクセスしない
3. 強固なパスワードを使う
4. セキュリティ対策ソフトを使う
5. パソコンだけでなく、スマホなども含めて対策
6. 盗難・紛失や廃棄時にも注意
7. 万一に備えてバックアップ

図3　サイバー犯罪に巻き込まれたくなければ、ここに挙げた7つの項目を守るようにしたい

●Windowsのサインインから安全対策

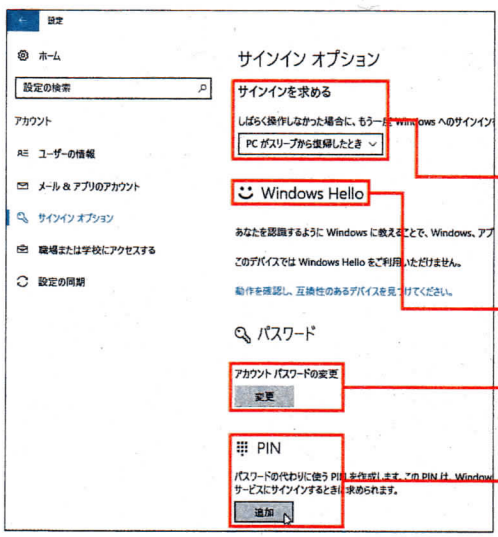


図4　Windows 10のアカウント設定では、各種のサインインオプションを設定できる。パソコンの使い方に応じて、適切なセキュリティ設定にしよう

●Windows 10最新版で機能強化

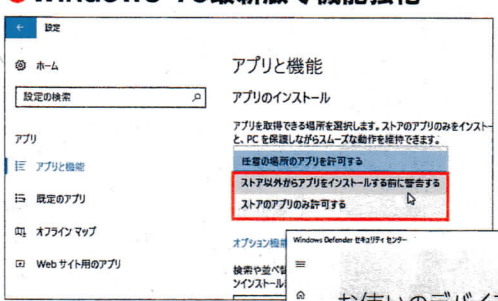


図5　最新版では「アプリと機能」の設定でストア以外からのインストールを警告したり、禁止したりできる

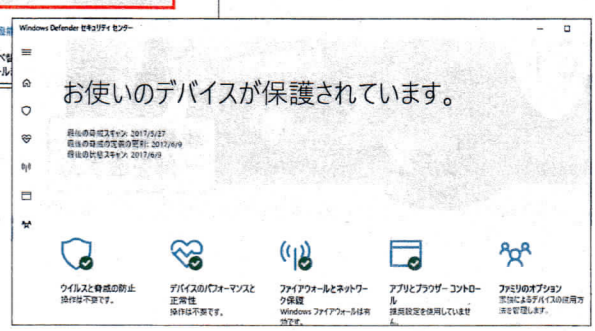


図6　最新の「Windows Defenderセキュリティセンター」では、ウイルス対策だけでなく、ファイアウオールなどのセキュリティ設定をまとめて管理できる

クリックしなくても感染!? 巧妙な手口の対処法

●広がるサポート詐欺

- 遠隔サポートすると偽り、不正ソフトをインストール
- サポート料金の不正請求
- 個人情報を盗む

対策

- 絶対に電話しない

図1　2016年くらいから増えてきた「サポート詐欺」。Webサイトを表示すると、いきなりセキュリティなどの警告が表示され、サポートへの電話を指示される

●進化するワンクリック詐欺

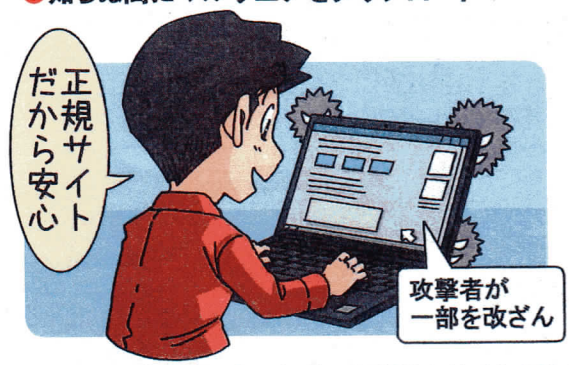
- 金銭を要求する
- 個人情報を盗む

対策

- 怪しげなWebサイトを見ない
- クリック前に要確認
- 請求表示は無視する

図2　アダルトサイトなどで動画や写真などをクリックすると金銭を要求されることで話題になった「ワンクリック詐欺」。クリックしなくても請求画面が表示されたり、無料ソフトのダウンロードに見せかけたワンクリック詐欺があったりと、より注意が必要になっている

●知らぬ間にマルウエアをダウンロード



- 個人情報を盗む
- 金銭を要求する
- 感染拡大の手助けをする

対策

- 広告などはクリックしない
- ソフトウエアを最新版にする
- 定期的にウイルスチェック

図3　大企業やメーカーなどの公式Webサイトを改ざんして、閲覧したユーザーのパソコンにマルウエアをダウンロードさせる「ドライブバイダウンロード攻撃」。自動的に偽サイトに誘導して強制的にダウンロードさせるなど、より分かりづらく、巧妙な手口になっている

「ウイルスに感染。すぐサポートにお電話を！」といった画面を表示させる「サポート詐欺」。慌てて電話をかけてしまうと、高額なサポート契約を迫られるといった事例が起こっている（図1）。不安につけ込む手口は、以前騒がれた「ワンクリック詐欺」より悪質だ。

変化する詐欺の手口

クリックするだけで不当な請求を受けるワンクリック詐欺（図2）。多少件数が減ったものの、Webサイトを開くだけで請求画面が表示される「ノークリック詐欺」など、より防ぎづらくなっている。

こうした被害の多くがアダルトサイトやギャンブルサイトといった怪しげなWebサイトで起こることに変わりはないが、大企業や公共機関のWebサイトにおいても危険はある。一般ユーザーが多く集まる場所は攻撃者にとって絶好のターゲット。知らぬ間に偽サイトに誘導されたり、マルウエアを仕掛けられたりするといった被害を耳にしたことがあるだろう（図3）。

ただ、だからといって「危なくて使えない」と考えるのは早計だ。最新の事情を知り、対策を取ることで、事前に回避したり、被害に遇ったとしても最小限に抑えたりすることはできる。

まず、突然表示される画面に慌てないよう、対処法を頭に入れておこう。こうした画面は無視するのが得

用語解説

Cookie
Webサイトを利用した際に、利用者側に保存されるデータ。情報を利用者の機器に保存しておくことで、利用者に合わせた設定でWebページを表示できる。

策。表示されたタブを閉じ、Webブラウザーを終了させ、ウイルス駆除を行う。再起動後、念のため履歴やCookie（クッキー）を削除する。それでも消えない場合は、下のコラムを参照して対処しよう。

ブラウザーの設定を見直す

悪質化する手口への対抗策も日々進化している。ソフトウエアを更新することで、WannaCryのような被害は避けられるのだ。

Webブラウザーを最新版に更新して、設定もこの機会に見直そう。グーグルの「Chrome」なら、「危険なサイトからユーザーとデバイスを保護する」にチェックが付いていることを確認する（図4）。不要なポップアップや広告をオフにするだけで、危険度はかなり下がる（図5、図6）。メールソフトやセキュリティソフトも最新版に更新しておこう。

それでもすり抜けてくるウイルスもあるので、定期的なウイルスチェックで駆除するのも忘れずに。

●Webブラウザーの設定を確認

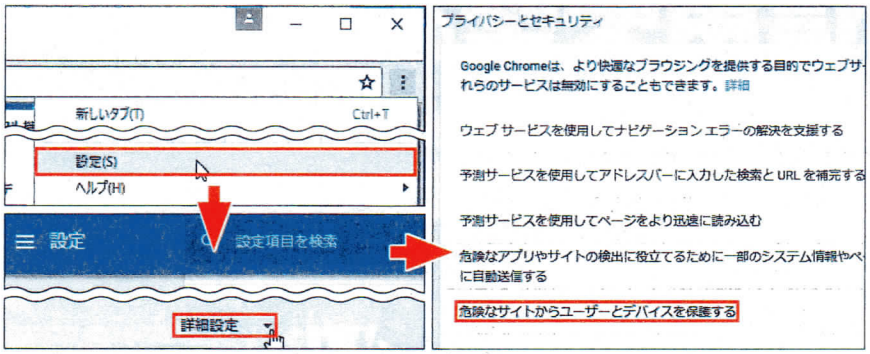


図4　Chromeのメニューから「設定」を選択（左上）。設定画面最下部の「詳細設定」を選択し（左下）、詳細設定画面で「プライバシー」の設定を確認（右）。「危険なサイトからユーザーとデバイスを保護する」には必ずチェックを付けよう

●ポップアップを表示させない

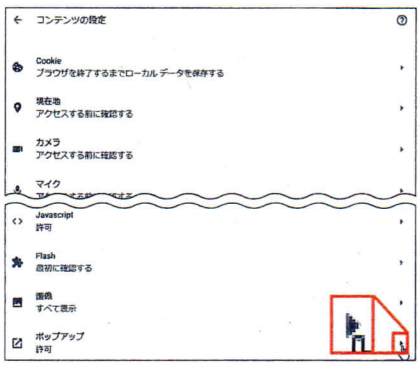


図5　図4の画面で「コンテンツの設定」をクリック。表示される画面では、CookieやJavaScript、ポップアップなどの設定を変更できる。変更するには右端の三角マーク（▶）をクリック

●広告を表示させない

図6　「Adblock Plus」などの拡張機能を使えば広告を非表示にできる。Chromeであれば、グーグルのWebサイト「Chromeウェブストア」からインストールする

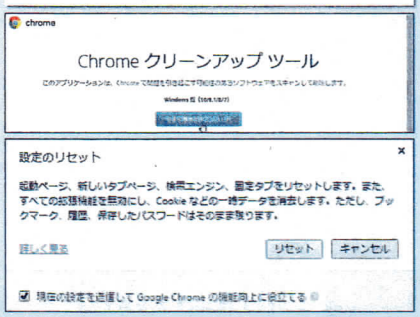
迷惑なポップアップが消せないときは

画面のクリックなどで表示されるワンクリックウエアの中には、パソコンを再起動しても消えないものもある。Chromeであれば、専用のクリーンアップツールを使ってみよう（図A）。また、ワンクリック詐欺専用の駆除ツールを使うという手もある（図B）。

攻撃者はさまざまな方法を開発してくる。「ホームページが勝手に変わった」といった怪しい動作をする場合、とにかく慌てないことだ。別のWebブラウザーやスマートフォンなどを使って似たような事例がないか検索し、正しい解除方法を探して対処しよう。

Chromeクリーンアップツール

提供元：グーグル
入手先：https://www.google.com/chrome/cleanup-tool/



図A　グーグルが提供する「Chromeクリーンアップツール」をダウンロード。確認画面で「リセット」をクリックする

ワンクリックウェア駆除ツール

提供元：cougar
入手先：http://fos.wp.xdomain.jp/

図B　どうしても消えない請求画面には、専用の駆除ツールもある。説明をよく読んで、使うかどうかを考えよう

楽しいはずのSNSが信用失墜の原因に

●アカウント乗っ取りはよくある会話から

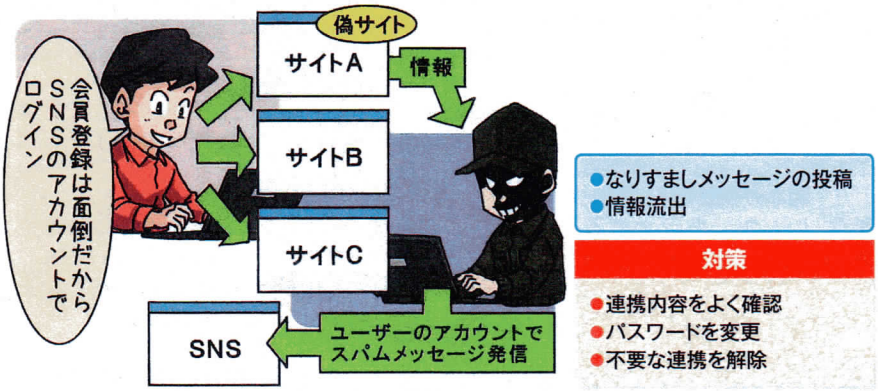
- なりすましメッセージの投稿
- 情報流出
- 友人への詐欺被害

対策

- アカウントにつながることを気軽に教えない
- 2段階認証を設定
- 乗っ取られたらすぐ通報

図1 「写真を送るから」などと、LINEなどのアカウントを聞かれるのはよくあること。しかし、相手によってはそれが乗っ取りのきっかけになることもある

●アカウントの連携で情報漏洩の危険



- なりすましメッセージの投稿
- 情報流出

対策

- 連携内容をよく確認
- パスワードを変更
- 不要な連携を解除

図2 Twitterなどのアカウントでログインできる Webサイトが増えている。よく確かめずに連携すると、情報漏洩などの危険がある

●「ここだけの話」がSNSで拡散

- ストーカー被害
- 情報流出

対策

- 発信している範囲を確認
- 個人情報はできるだけ書かない

図3 自分のフォロワーに向けて発信しているつもりでも、リツイートなどでネズミ算式に情報が拡散する恐れがあることを忘れてはいけない

LINEのアカウント乗っ取りが世間を騒がせたのは2014年のこと。その後もFacebookやTwitterなどSNSアカウントの乗っ取り事件は後を絶たない。個人情報が流出するだけならまだしも、友人にプリペイドカードを買わせるといった被害が出れば信用問題だ。

情報漏洩は油断から

よく知らない相手に電話番号は教えなくても、SNSのIDなら教えるという人は多い（図1）。しかし、SNSではプロフィールで、ある程度の個人情報が分かる。誕生日を非公開にしていても、友人からのお祝いメッセージで分かってしまう。家族が投稿した写真で居場所が分かるなど、SNSから流出する情報は多い。誕生日などからパスワードを推察され、アカウントが乗っ取られることがあるので、単純なパスワードは要注意だ。

TwitterなどのSNSアカウントでログインできる「アカウント連携」は、登録する手間が省けて便利だが、うっかり攻撃者の偽サイトにログインしてしまえば、連携している全てのサービスが危険にさらされてしまう（図2）。

SNSで仲間とメッセージをやり取りしていると、仲間にしか見えていないような錯覚を持つかもしれないが、その空間が世界中に広がっていることを頭に置いておこう。「ここだけの話」と思って個人的なことや他人の陰口を書くと、シェアやリツ

用語解説

リツイート▼
Twitterでほかのユーザーの投稿内容を再投稿すること。注目すべき投稿や興味深い投稿を、自分をフォローしているユーザーに紹介するなどの目的で行われる。

イートなどの機能で拡散されることもある（図3）。メッセージやプロフィールは公開範囲を指定しない限り誰でも見られることも忘れてはいけない。

情報の広がりを意識する

しかし、誰が見るか分からないからと、怖がる必要はない。個人的な話はメールや電話を使い、SNSでは「多くの人に見てほしい」情報を発信するのがお勧めだ。ストーカー被害などに遭う危険があるなら、「今ココ」といった情報を控え、時間をずらして書くなどの配慮をしたい。

SNSでは、メールアカウントをIDとして利用するサービスもある。メールアカウントが流出すればSNSも危険なので、定期的に流出をチェックしたい（図4）。万一流出しているようならパスワードやアドレスを変更する。SNS用にはフリーメールのアドレスを使い、通常のメールアドレスは外に出さないといった対策も有効だ。

アカウントの連携を使う場合は、画面をしっかり確認する（図5）。動画を見るサービスなのに位置情報や書き込みの許可が含まれるといった違和感があれば、連携を避けるのが賢明だ。確認画面を表示させない悪質なサービスもあるので、SNSで連携をチェックし、使っていないサービスは解除しよう（図6）。

自分が発信するメッセージやプロフィールの共有範囲を把握するのも大切だ（図7、図8）。それでもアカウントの乗っ取り被害に遭った場合は、速やかに運営側や友人に通知し、被害を最小限に抑えよう。

●メールアカウントの流出をチェック

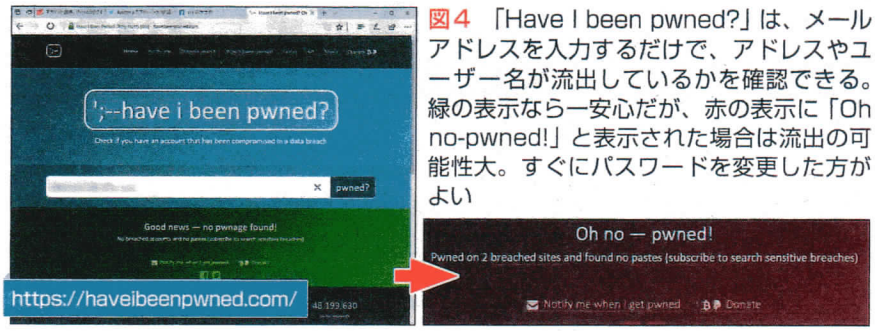


図4　「Have I been pwned?」は、メールアドレスを入力するだけで、アドレスやユーザー名が流出しているかを確認できる。緑の表示なら一安心だが、赤の表示に「Oh no-pwned!」と表示された場合は流出の可能性大。すぐにパスワードを変更した方がよい

●アカウント連携前のチェックポイント

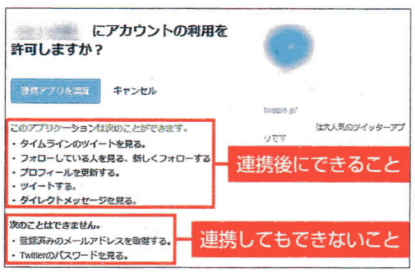


図5　SNSアカウントで別のアプリを使う場合、連携の認証画面をよく確認する。連携後にできることの中に、そのアプリで不要な機能が含まれている場合は要注意だ

●不要なアカウント連携を解除

図6　Twitterの場合、アカウントのアイコンをクリックして「設定とプライバシー」を選択。「アプリ連携」で、連携しているアプリを確認する。不要なアプリは「許可を取り消す」をクリックし、悪意のあるアプリの場合は「アプリを報告」で通報する

●プロフィールやメッセージの公開範囲を確認

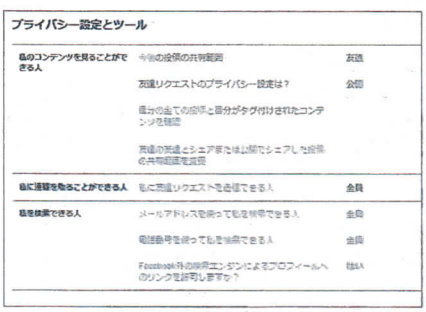


図7　Facebookでは、設定画面の「プライバシー」でメッセージの共有範囲などを設定できる。公開範囲が狭いほど安全性は高くなる

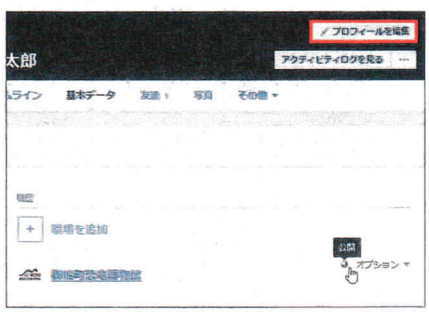


図8　個人情報の公開範囲を確認するには、自分のタイムラインを表示する。「プロフィールを編集」をクリックすると、職歴などの公開範囲を変更できる

Part 4 パスワード

セキュリティの第一歩 パスワード管理の常識

ドアに付けた鍵が多ければ、それを破ろうとする侵入者は激減する。なぜなら、鍵を掛けない家や、鍵が1つだけの家を狙う方が効率が良いからだ。パスワードも同じこと。強固なパスワードにすれば、破られるリスクを低減できる。

とはいえ、利用しているWebサービスが多いと、全サービスのパスワードを見直すのは難しい。そこで、パスワードの見直しは、Webサービスのグループ分けから始めるのがお勧めだ(図1)。

簡単に安全を手に入れる

利用しているWebサービスごとに重要度を考えて分類する。重要度が低いサービスは、簡単なパスワードでも大きな問題にはならない。

銀行や買い物などのお金がからむWebサービスは、狙われる可能性が高く、金銭的な被害に直結するので重要度は「高」。無料のニュースサイトのように「見るだけ」のサービスは、重要度「低」でよいだろう。

グループ分けができたら、重要度の高いWebサービスから、パスワードを強化していこう。

短く、単純なパスワードや、誕生日などから連想できるパスワードは、すぐ突破されてしまう(図2)。文字数や文字種を増やすほど破られにくくなるのだが、作るのも覚えるのも面倒になっては困る。

Webサービスごとに、複雑でも覚えやすいパスワードを作るコツは、自分だけのルールを決めることだ。

例えば、好きな言葉と数字を組み合わせて基本パスワードを作り、記号とWebサービスの略号で挟み込む(図3)。最後に設定月を付ければ、定期的に更新するのも楽だ。

図3のパスワードが流出した場合、「FacebookがFBなら、TwitterはTWか」などと、別のWebサービスのパスワードを連想される危険性が

●Webサービスの重要度を考えてグループ分け

高	中	低
オンラインバンキング ネットショッピング オンライントレード など	SNS、ブログ メール 有料サービス など	ニュース 企業サイト 友人のブログ など

図1 パスワードが必要なWebサービスにもいろいろある。盗まれると被害の大きいパスワードは使い回さないなど、ルールを決めよう

●「弱いパスワード」と「強いパスワード」

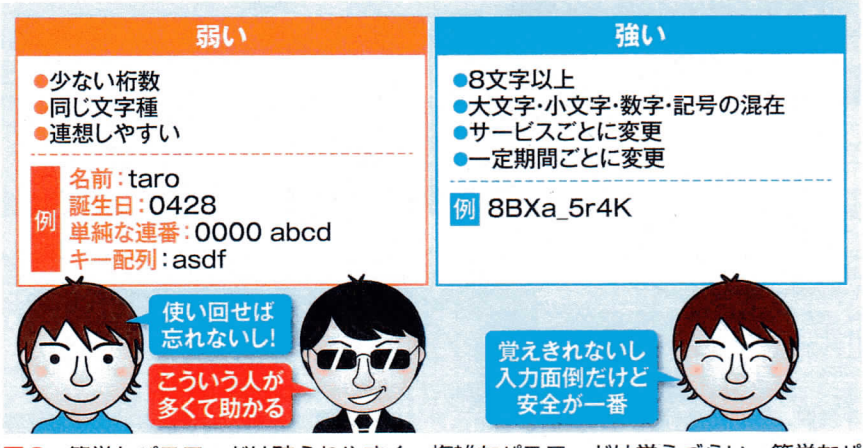


図2 簡単なパスワードは破られやすく、複雑なパスワードは覚えづらい。簡単なパスワードを使い回せば、攻撃者にとって絶好のターゲットになることは間違いない

●複雑でも覚えられるパスワードを考える

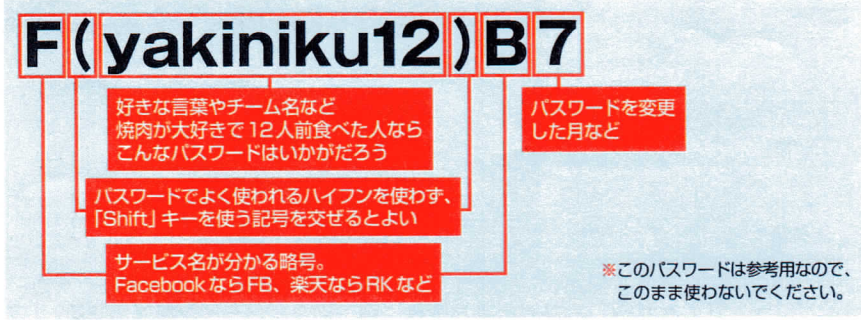


図3 「強い」パスワードは覚えづらいものだが、自分なりの法則を作ることで「覚えられるパスワード」を作れる

ある。重要度の高いWebサービスにはもう一工夫必要だが、ルールを決めておけば長い文字列でも覚えられることが分かるだろう。

パスワードの入力を簡略化

パスワードの文字数を増やすほど、強度は上がるが入力が面倒になる。Webブラウザーには、パスワードを保存し、自動入力する機能があるので、利用している人も多いだろう(図4)。便利な機能だが、Windowsのパスワードさえ分かれば、ほかの人でも保存したパスワードは見放題だ(図5)。重要度の低いサービスのパスワードのみ保存するなど、便利さと安全性のバランスを考えたい。

Webブラウザーが「Firefox」の場合、「マスターパスワード」を設定すると、保存したパスワードの使用時にマスターパスワードの入力を求められるため、安全性が上がる(図6)。

Chromeなど、マスターパスワードのないWebブラウザーでパスワードを自動入力させたいなら、パスワード管理ソフトを使った方がよい。例えば「LastPass」(無料版)では、Webサービス利用時に入力したパスワードを保存し、自動入力してくれる(図7)。指紋認証やマスターパスワードにも対応しており、パスワードは暗号化してクラウドに保存。スマートフォンや外出先でも利用でき、ファイルの流出時やパソコンが壊れた場合でもパスワードを守れるのもメリットだ。

Googleなどの大手のWebサービスでは、パスワードを二重に掛ける「2段階認証」に対応しているので利用したい(図8)。

●Webブラウザーに保存したパスワードを確認

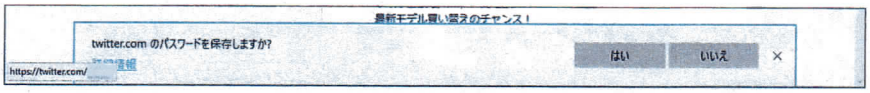


図4　パスワード入力時、Webブラウザーに保存するかどうかを聞かれる

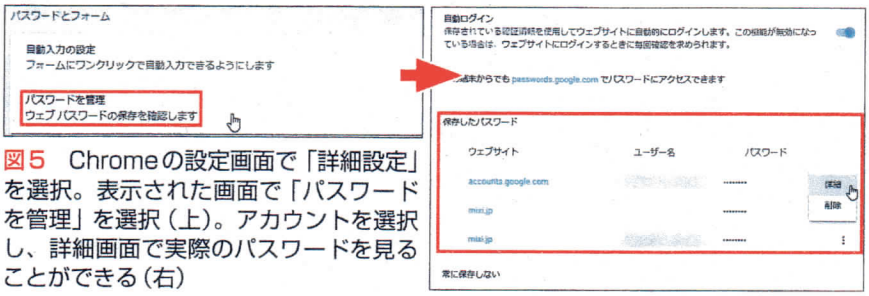


図5　Chromeの設定画面で「詳細設定」を選択。表示された画面で「パスワードを管理」を選択(上)。アカウントを選択し、詳細画面で実際のパスワードを見ることができる(右)

●「Firefox」ならマスターパスワードを設定

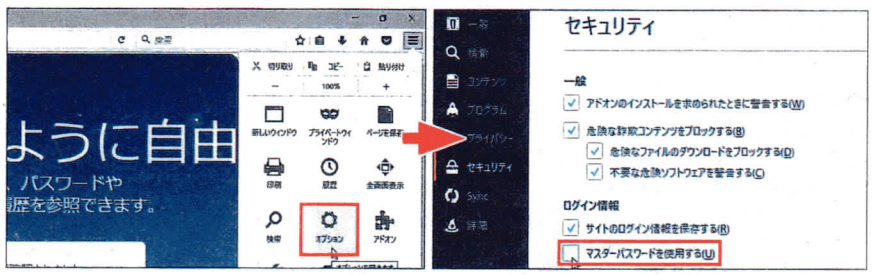


図6　Firefoxのメニューから「オプション」を選択。「マスターパスワードを使用する」を選択して設定する

●パスワード管理ソフトを利用

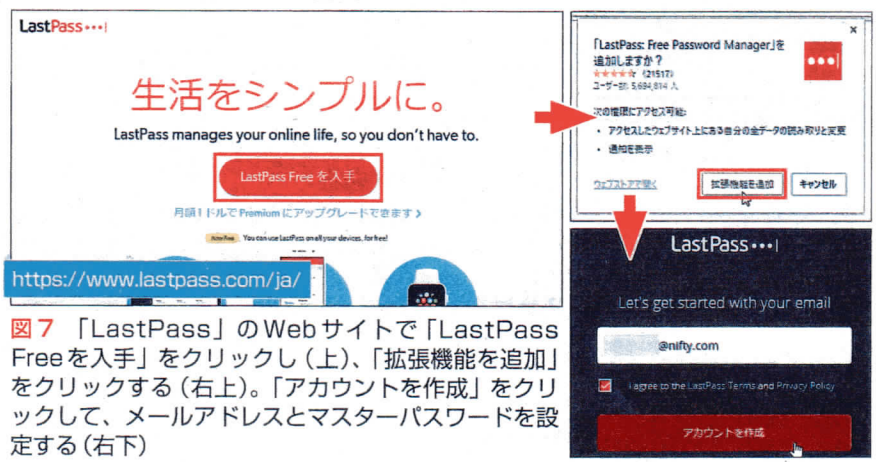


図7　「LastPass」のWebサイトで「LastPass Freeを入手」をクリックし(上)、「拡張機能を追加」をクリックする(右上)。「アカウントを作成」をクリックして、メールアドレスとマスターパスワードを設定する(右下)

●2段階認証で安心度アップ

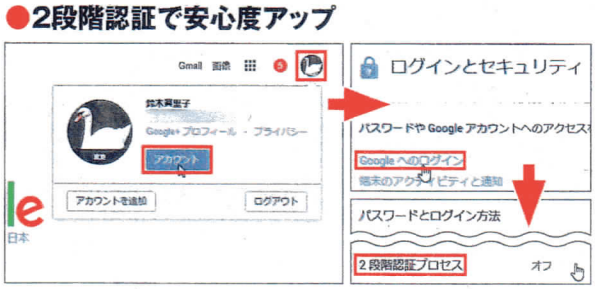
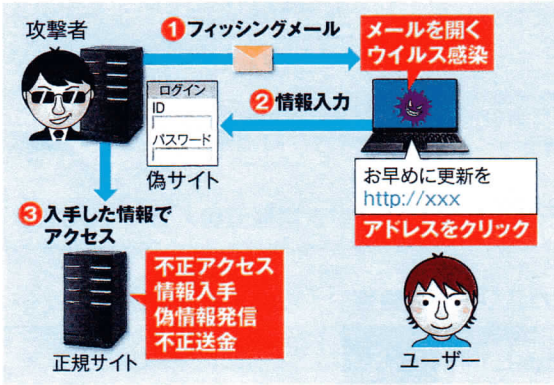


図8　Googleのアカウントアイコンをクリックし、「アカウント」をクリック(左)。「Googleへのログイン」をクリックして(右上)、「2段階認証プロセス」の設定を行う(右下)

「怪しくないメール」ほど注意が必要

●根強く残るフィッシング詐欺



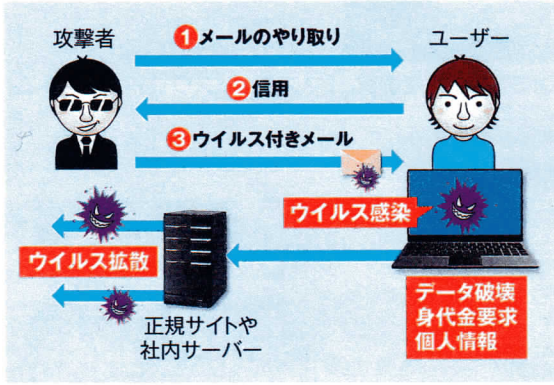
- 情報漏洩
- 不正アクセス
- 偽情報発信
- 不正送金
- ウイルス感染

対策

- 怪しいメールや添付ファイルを開かない
- メール内のアドレスにアクセスしない
- ウイルス対策を行う

図1　メールを開いたり、メール内のアドレスをクリックしたりすることで、サイバー犯罪に巻き込まれるフィッシング詐欺

●標的型攻撃メールとは



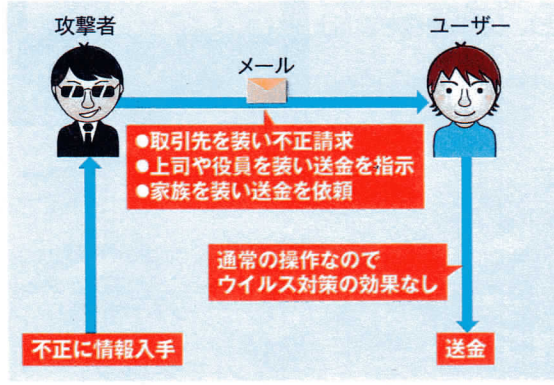
- ウイルス感染
- 情報漏洩
- データ破壊
- 身代金要求
- ウイルス拡散

対策

- メールの内容をよく確認する
- ウイルス対策を行う

図2　不特定多数ではなく、対象の人物や組織を絞って巧妙に仕組まれたウイルス付きメールは、見破るのが難しい

●BEC詐欺（メール版振り込め詐欺）



- 不正送金
- 情報漏洩

対策

- メールの内容をよく確認する
- 送金前に本人確認を行う

図3　関係者を装い、送金を促すメールを送付する詐欺。偽装サーバーなどを使う手口と違って送金自体は通常の操作なので、ウイルス対策などは効果がない

トレンドマイクロの調査では、ランサムウエア（身代金要求型不正プログラム）の拡散を目的とした攻撃の79%がメールを利用しているという。セキュリティを考える上で、メールへの対策は欠かせない。

巧妙化する詐欺手口

攻撃者からのメールをうっかり開いたり、メールに書いてあるアドレスをクリックしたりといったことで被害に遭う「フィッシング詐欺」（図1）。数年前なら外国語のメールや「500万円当選」といった怪しげなメールに注意すればよかったが、最近の偽装は巧妙だ。

入手した個人や企業の情報を使ってピンポイントで狙ってくる「標的型攻撃メール」では、何度かのやり取りで信用させてからウイルスを仕込む（図2）。添付されるウイルスも文書やPDFに加工されているので分かりづらい。

最近増えてきたのが、取引先や上司を装う「BEC（Business E-mail Conpromise）詐欺」（図3）。経理担当者に取引先を装って「口座が変わりました」といったメールを送るなど、文面もよく考えられている。企業ではこうした詐欺が流行していることを周知し、確認を徹底しよう。

メールを開くだけでもウイルスに感染することがあるので、メールソフトのプレビュー機能はオフにするのが基本（図4、図5）。開いたメールは内容をよく確認する（図6）。メ

用語解説

プレビュー▼
処理の結果を、実行前に確認すること。メールソフトの場合、メールを選択しただけで本文や添付ファイルの内容を表示するプレビュー機能を備えるものがある。

ールで指示されたURLにアクセスする必要がある場合、クリックするのではなく、Webブラウザーで手入力し、安全性を確認してから情報を入力する(図7、図8)。

ごく普通のやり取りを装う詐欺メールを見破るのは難しい(図9)。企業はもちろん、個人でもセキュリティ対策ソフトの導入が望ましい。

●「開かない」ためにプレビューを「オフ」

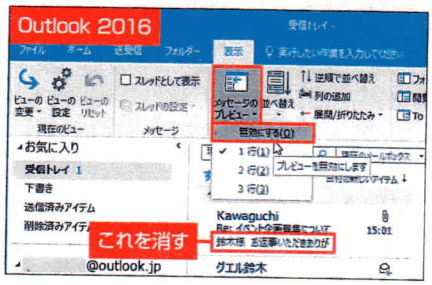


図4 「表示」タブの「メッセージのプレビュー」を「無効にする」を選択する

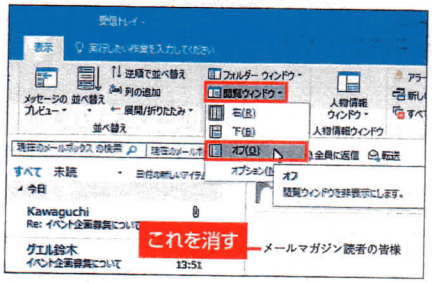


図5 「表示タブ」の「閲覧ウィンドウ」を「オフ」にして、プレビュー画面を消す

●フィッシングメールの例

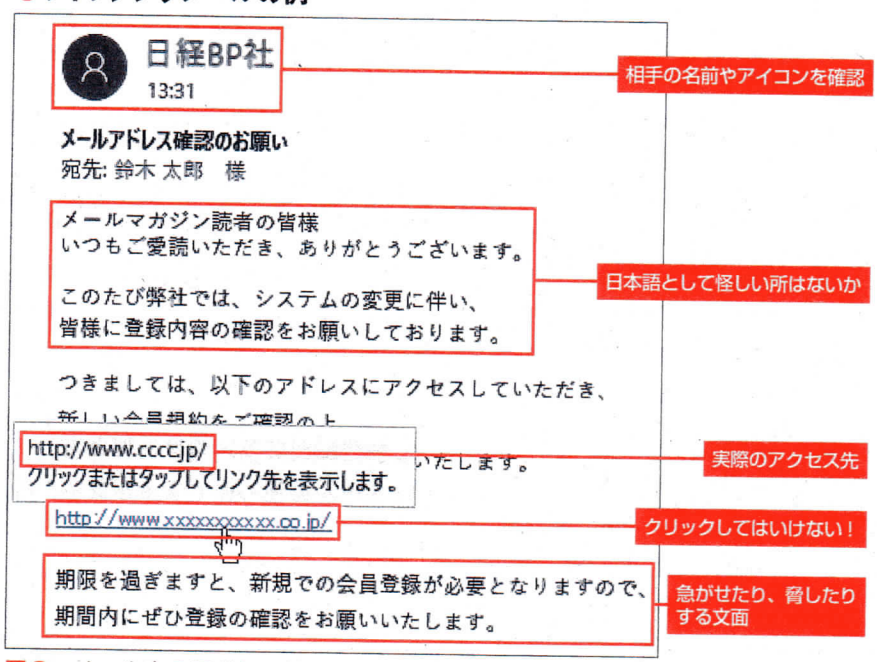


図6 メール内のアドレスはクリックしないのが原則。特に表示しているURLと、マウスを合わせたときに表示される実際のアクセス先が異なる場合、フィッシングの可能性が高い

●入力前、アクセス前に確認

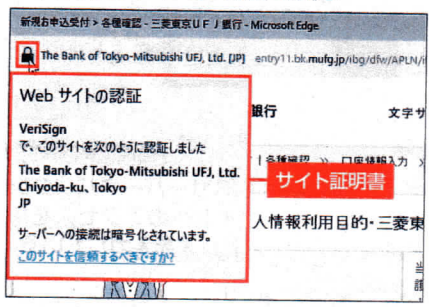


図7 Edgeでは、暗号化を示す鍵のマークをクリックすると証明書が見られる

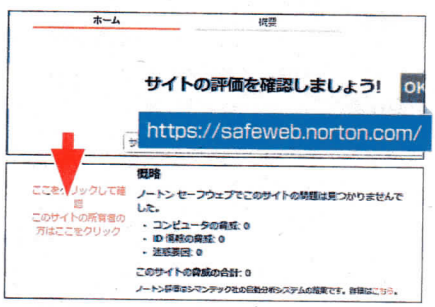


図8 シマンテックの「Safe Web」は、アドレスで安全性を確認できる

●段階を踏んでわなを仕掛ける標的型攻撃メール

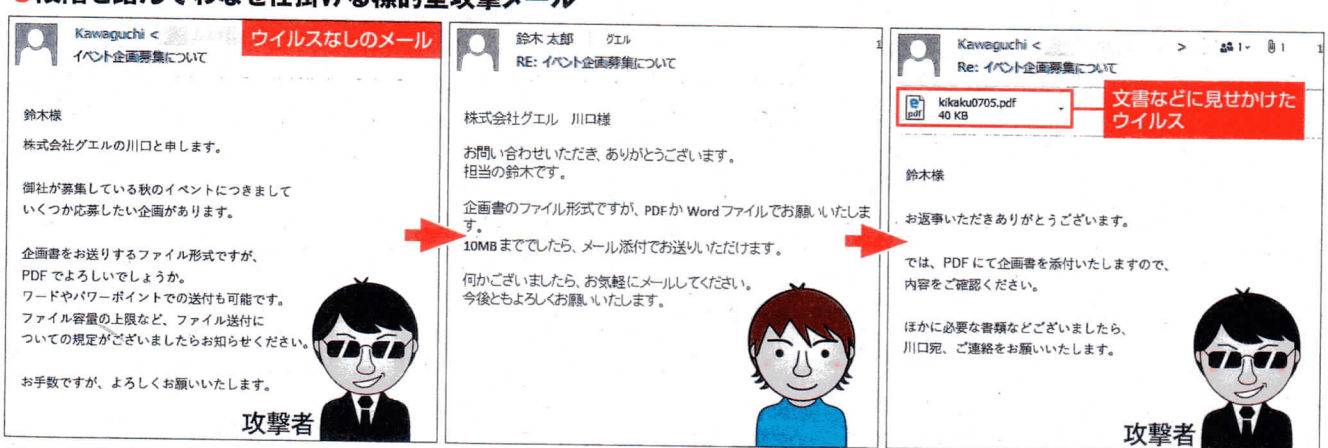


図9 標的型攻撃メールでは、最初に何度か安全なメールのやり取りをして信用させ、最後にウイルス付きのメールを送ってくる

巧妙になるサイバー攻撃 ポイントは二重、三重の防御

●DNSサーバーを攻撃して偽サイトに誘導

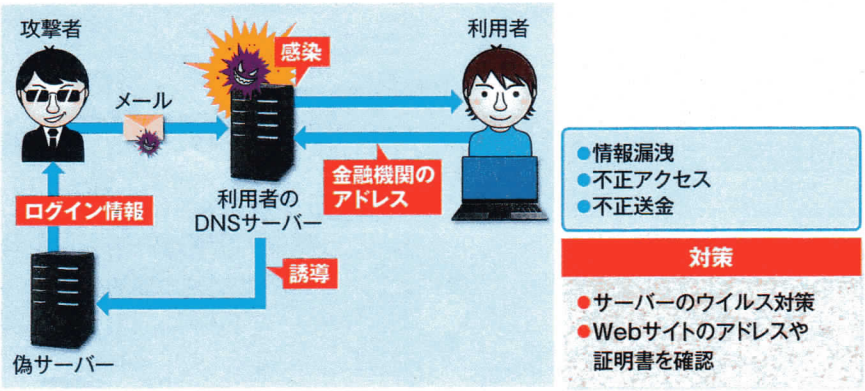


図1　利用者のDNSサーバーやパソコン内の「hosts」というファイルにウイルスを感染させ、正規サイトへのアクセスを待って偽サイトに誘導する「ファーミング」。利用者は正規のアドレスを入力しているので疑わないことも多い

●Webブラウザーを攻撃して不正送金

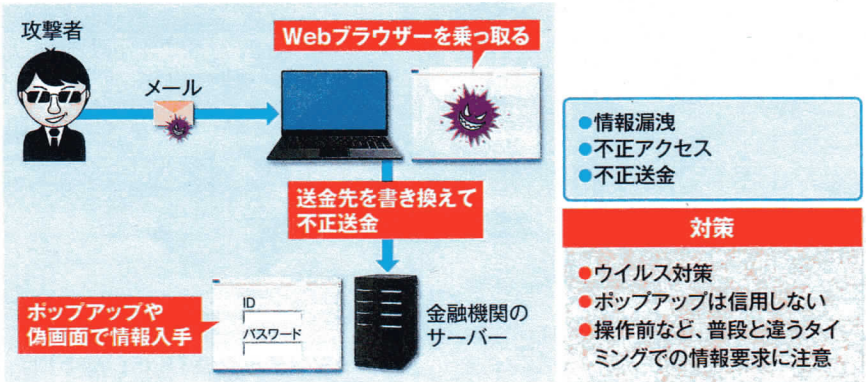


図2　「MITB（マン・イン・ザ・ブラウザー）」と呼ばれる攻撃では、利用者のWebブラウザーを攻撃し、金融機関へのアクセスを感知してWebページを自動的に書き換える。ログイン情報の入手や、送金先を書き換えて不正送金が行われる

●巧妙なフィッシングメール・偽サイト

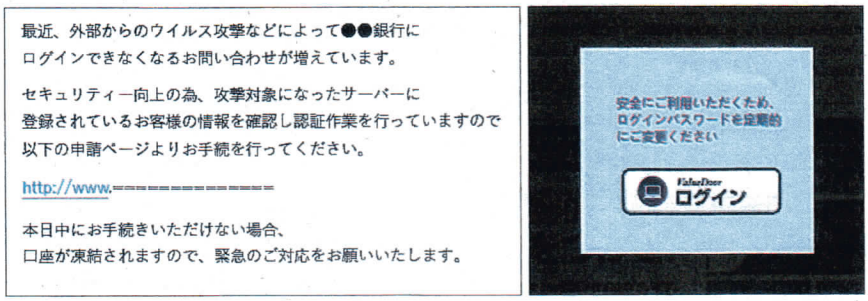


図3　金融機関を装う偽メールや偽サイトは、より巧妙に作成されている。本物と見分けがつかないこともあるので、注意が必要だ（右の画面はみずほダイレクトのWebサイトに掲載されているイメージ）

警察庁によれば、平成27年におけるインターネットバンキングの不正送金被害額は30億円を超え、半分以上が個人の被害だ。法人は対策が進みつつあるものの、個人についてはいまだに管理が甘いことが指摘されている。平成28年上半期の個人の被害額は、実に全体の75%を占めている。銀行をはじめ金融に関わるオンライン取引は金銭の被害に直結するため、攻撃者のターゲットになりやすく、利用者はより慎重な対応をしなくてはならない。

さまざまな攻撃手段

金融関係のオンライン取引における情報漏洩で多いのは、何と言ってもメールを使った「フィッシング詐欺」だ。メールに記載したURLで偽サイトに誘導し、パスワードなどを盗み取る。

メールのURLはクリックしない、という人でも引っ掛かるのが「ファーミング」だ（図1）。利用者のパソコンやDNSサーバーにウイルスを仕掛け、偽サイトに誘導する。利用者はいつものURLにアクセスしたつもりでも、いつの間にか偽サイトでパスワードを入力してしまうから厄介だ。大事な情報の入力前には、再度アドレスを確認するといった慎重さが求められる。

正しい金融機関のWebサイトであっても不正画面が表示される「MITB攻撃」（MITB=Man in the Browser）は、見破るのが難しい（図

用語解説

DNSサーバー▼
「www.nikkeibp.co.jp」などのドメイン名と、「202.214.174.229」などのIPアドレスを相互に変換する機能を提供するインターネット上のサーバーのこと。

トークン▼
ユーザー認証に必要な情報を格納したハードウエアなどを指す。認証が必要なログイン時などに、パソコンにトークンを接続してユーザー認証を行う。

2)。ウイルスで書き換えられたWebブラウザーが金融機関へのアクセスを関知して、偽画面で情報を流す。Webブラウザーの設定でポップアップ画面をオフにし、セキュリティ対策ソフトを使って防御しよう。

フィッシング詐欺のメールがさらに巧妙になっていることにも注意したい。「口座に不正なアクセスがあった」といった利用者の不安を突いたメールで、本物そっくりの偽サイトに誘導する(図3)。

金融機関の対策を利用

利用者の注意力だけでは対応しきれないこうした犯罪に、金融機関も手をこまねいているわけではない。最新の情報を提供するだけでなく、さまざまな対策を行っている(図4)。金融機関によっては複数の対策を用意しているので、利用者の環境に合わせた対策を取り入れたい。

取引ごとや一定時間ごとに使い捨てのパスワードを発行する「ワンタイムパスワード」は、パスワードを盗まれても長期間使用できないといった利点がある。以前は専用カードやトークンといった専用機器を貸し出していたが、有料であり、一般の利用者には敷居が高かった。最近ではスマートフォンを使ったアプリとして無料で提供する機関が増えている(図5)。アプリによっては、取引時にパスワード入力を自動で行う機能があり、安全性も利便性も高い。

オンライン取引専用のウイルス対策ソフトを配布する金融機関も多い(図6)。オンライン取引に特化したソフトだ。市販のセキュリティ対策ソフトと併用するとよいだろう。

●金融機関が取り組むサイバー犯罪対策

ワンタイムパスワード	1回限りの使い捨てパスワードを発行する機器やアプリを提供
メール通知	振り込みなど、重要な取引の場合、取引があったことを通知するメールを送付
第2暗証番号の入力	振り込みなど、重要な取引の場合、二重の暗証番号で保護
ログイン画面の画像変更	ログイン画面の画像を選択することで、偽サイトと区別
合言葉	通常とは異なる環境からアクセスされた場合、秘密の質問などを使って追加認証
専用ウイルス対策ソフト	オンラインバンキング専用のウイルス対策ソフト(Rapport、PhishWallなど)を配布
利用する機器の登録	パソコンなど、取引に利用する機器をあらかじめ登録

図4　年々巧妙になるサイバー犯罪に対応するため、金融機関では複数の対策を用意している。いくつか組み合わせることで、より強固な対策となる

●スマホ用ワンタイムパスワードアプリが登場

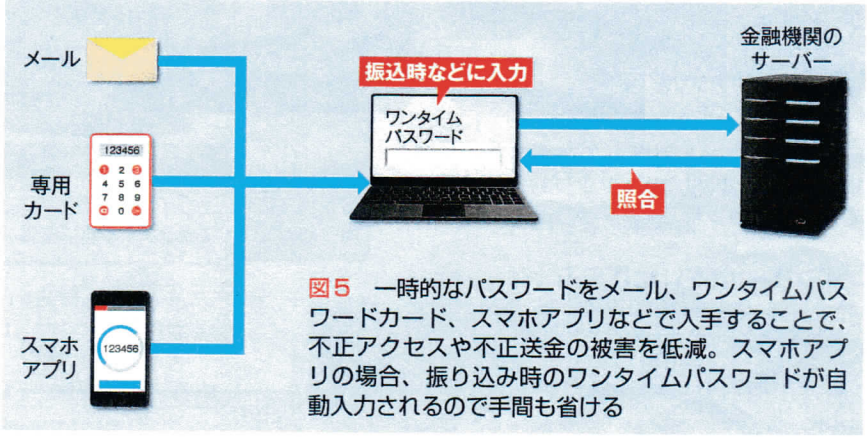


図5　一時的なパスワードをメール、ワンタイムパスワードカード、スマホアプリなどで入手することで、不正アクセスや不正送金の被害を低減。スマホアプリの場合、振り込み時のワンタイムパスワードが自動入力されるので手間も省ける

●金融機関で無料配布する専用のウイルス対策ソフト

図6　銀行などの金融機関の多くは、オンラインバンキング専用のウイルス対策ソフトを無償で提供している。正規Webサイトからダウンロードできる

モバイル機器は「無料」が危ない

●スマホも危険！　ワンクリック詐欺

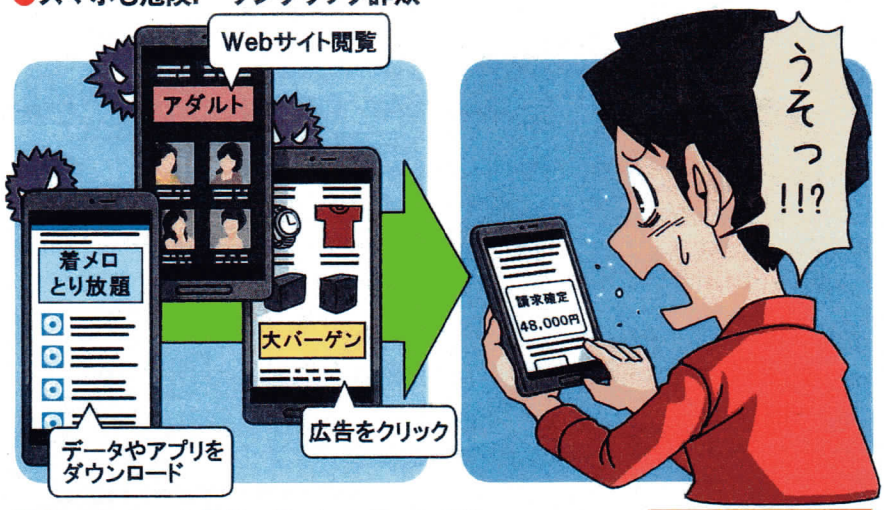


図1　パソコンと同様、スマートフォンでもWebサイトを開いたりタップしたりすることで感染するランサムウエアがある

●金銭要求
●情報漏洩

対策
●ウイルス対策
●タップする前に確認

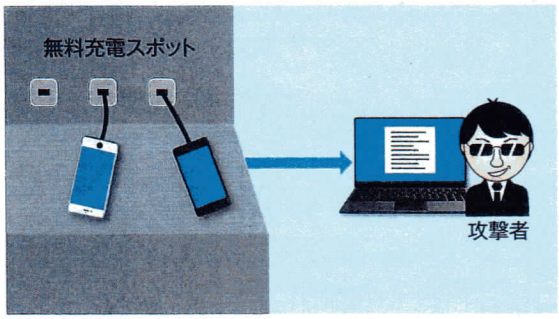
●「フリーWi-Fi」にご用心

●偽サイトへ誘導
●情報漏洩

対策
●ウイルス対策
●タップする前に確認

図2　無料Wi-Fiスポットによっては、通信情報を暗号化していないところもある。同じWi-Fiスポットに接続している人に情報を盗まれたり、ウイルスによって偽サイトに誘導されたりする危険性がある

●無料充電スポットから情報漏洩



●情報漏洩

対策
●USBの無料充電スポットは使わない
●充電の際はスマホの電源を切る

図3　繁華街などにある無料の充電スポットは便利だが、USBでの接続には危険が伴うことを覚えておこう

スマートフォン（スマホ）やタブレットを狙うサイバー犯罪は増加傾向にある。持ち運ぶノートパソコンを含めて、モバイル機器特有の対策についても検討しておこう。

外出先の「接続」に要注意

モバイル機器でもパソコンと同様のワンクリック詐欺やフィッシング詐欺が増えている（図1）。モバイル機器では迷惑メール対策が不十分なことが多く、うっかりボタンに触れてしまう危険性も高い。怪しげなメールや広告は触らないよう、注意したい。

モバイル機器ならではの危険も多い。紛失や盗難、肩越しにパスワードを盗まれる「ショルダーハック」などが代表的だが、あまり知られていないのが無料スポットでのウイルス感染だ。

外出時にWi-Fiをオンにしておくと、自動的に無料Wi-Fiスポットに接続されることがある。攻撃者が設置しているWi-Fiスポットに接続してしまえば、ウイルスに感染したり、同じWi-Fiスポットに接続している別の機器から情報を盗まれたりすることも考えられる（図2）。

充電が切れそうなときに便利な無料充電スポットも要注意だ（図3）。カスペルスキーの調査によれば、USB経由で充電スポットに接続しただけでウイルスに感染する可能性が指摘されている。また、充電元が電源ではなくパソコンだった場合、

用語解説

キャッシュ▼
アクセスしたWebページをファイルとしてパソコン側に保存するWebブラウザーの機能のこと。いったん表示させたWebサイトの再表示が素早くなる。

USB経由でデバイス名やメーカー名、シリアルナンバー、機種によってはOS情報やファイルリストまで読み取ることが可能だという。外出先での充電は、信頼できる場所に限定し、充電時は機器の電源を切るといった予防策が有効だ。

やっておきたい予防策

スマホなどで動画や音楽を楽しむ際、専用のアプリをインストールするよう求められることがある。こうしたアプリの中には、個人情報を盗もうとするものがあることを覚えておこう(図4)。

もしも金銭要求などの画面が表示されてしまったら、Webブラウザーのタブを閉じ、キャッシュクリアなど痕跡を消す操作を行う(図5)。

外出先でWi-Fiスポットを利用する場合、通信が暗号化されないスポットは傍受される危険性がある。鍵のマークがないスポットや怪しげなWi-Fiには自動接続しないよう、削除しておこう(図6)。Wi-Fiスポットが見つかるたびに表示されるポップアップが気になるなら、「接続を確認」をオフにしておけばよい。

スマホのパスコードがいまだに4桁の数字という人は、設定を変更して、英数字を組み合わせたより強固なパスコードにして安全性を高めるべきだ(図7)。

●アプリはインストール時に注意

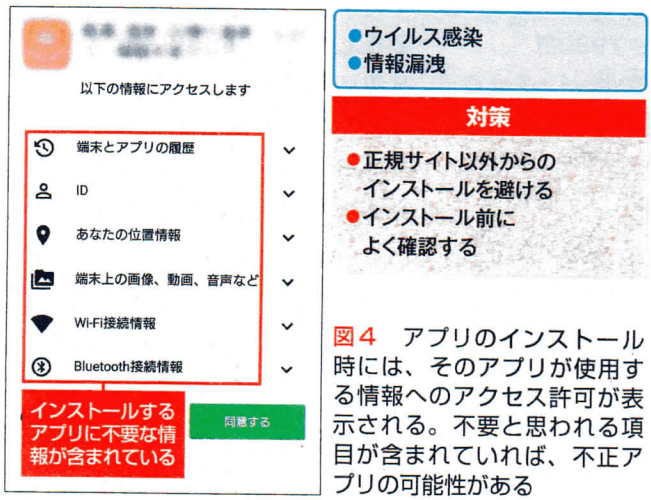


図4　アプリのインストール時には、そのアプリが使用する情報へのアクセス許可が表示される。不要と思われる項目が含まれていれば、不正アプリの可能性がある

●ワンクリック詐欺の画面が表示されたら

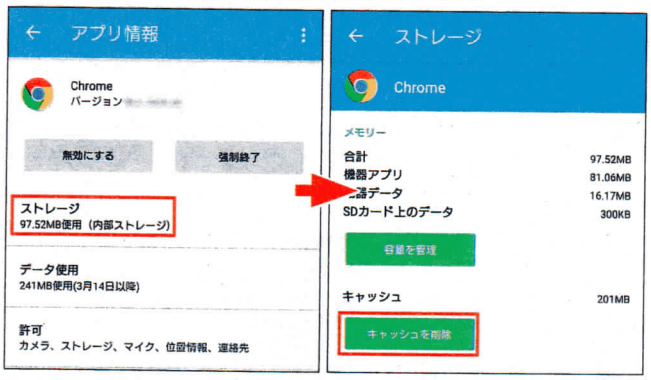


図5　請求画面が表示されたときには、ボタンなどをタップせず、Webブラウザーのタブを閉じる。その後、使用していたWebブラウザーの設定画面を表示し、キャッシュをクリアすると、請求画面を消せる可能性が高い(画面はAndroid)

●怪しいネットワークに自動接続させない

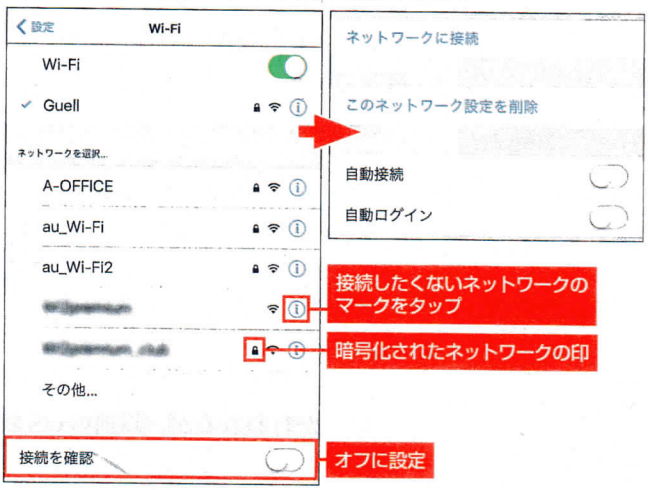


図6　iPhoneの場合、Wi-Fiの設定画面で接続したくないネットワークの「i」マークをタップする。表示された画面で設定を削除するか、自動接続をオフにする。「接続を確認」をオフに設定すれば接続の確認も表示されなくなる

●パスコードをより強力にする

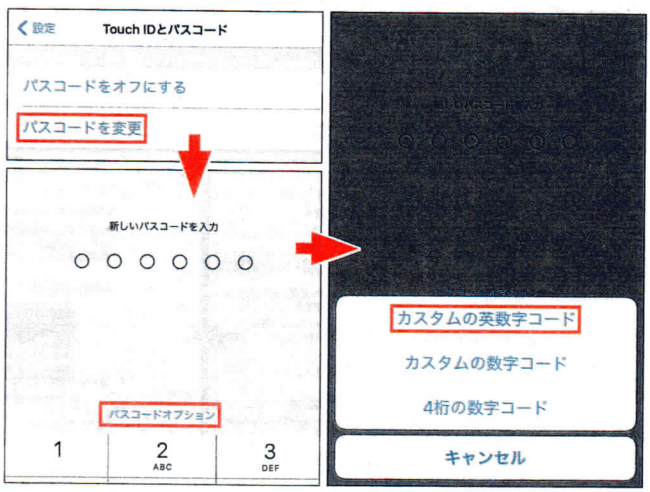


図7　iPhoneの設定画面で「Touch IDとパスコード」→「パスコードを変更」→「パスコードオプション」と選択。「カスタムの英数字コード」を選択すれば、アルファベットもパスコードとして使える

Part 8 対策

最新のサイバー犯罪への備えを再点検

●スマホにも対応したセキュリティ対策ソフト

シマンテック
ノートン セキュリティ デラックス

豊富な機能を簡単な設定で実現。お任せの設定で使用できるので、パソコンに詳しくない人も安心。ウイルスを駆除できない場合は全額返金保証、「クレジットカードの不正使用保険　年間最高100万円」も付属

直販価格(税込):1年3台 5918円
https://www.nortonstore.jp/

トレンドマイクロ
ウイルスバスター クラウド

偽サイトをブロックする「セキュリティ証明書チェッカー」。改ざんされた正規サイトや不正広告などをブロック。OneDrive上のファイルをスキャンする「クラウドストレージスキャン」など、機能が充実

直販価格(税込):1年3台 7980円
http://safe.trendmicro.jp/

マカフィー
マカフィー インターネットセキュリティ

台数無制限が魅力。顔認証でのパスワード管理が楽。Apple Watch サポート、迷惑電話やSMSの着信拒否など、スマホやタブレット向けの機能も豊富。モバイル機器の紛失／盗難時に役立つ

直販価格(税込):1年台数無制限 7180円
https://www.mcafee.com/

カスペルスキー
カスペルスキー セキュリティ 2017

ウイルス検知の正確さやファイアウオールの強固さに定評のあるソフト。強力なネットバンキング保護や新機能の「ソフトウェアアップデーター」など、新たな脅威への備えにも力を入れている

直販価格(税込):1年5台 4980円
http://home.kaspersky.co.jp/

図1　パソコンだけでなく、スマホやタブレットのサイバー犯罪を防ぐには、複数台での使用が可能なセキュリティ対策ソフトを利用したい。インストールする台数や必要な機能を考えて選ぼう

●Windows 10以外は「Windows Update」を自動更新に

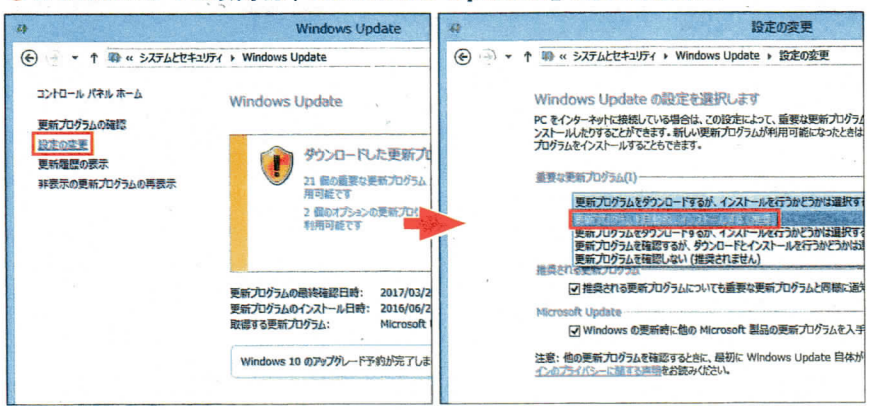


図2　コントロールパネルの「システムとセキュリティ」で「Windows Update」を選択。「設定の変更」を選択して(左)、「更新プログラムを自動的にインストールする」を選択する(右)

最後に、サイバー犯罪全般に有効な対策を見直そう。被害に遭う前に、ぜひ導入を検討してほしい。

Windowsの設定から見直し

Windows 10には、「Windows Defender」などのセキュリティ対策ソフトが付属しているが、それだけで十分とはいえない。より高い安全を考えるなら、市販のセキュリティ対策ソフトの導入を検討しよう。

市販のセキュリティ対策ソフトはWebサイトの改ざんやフィッシングサイトの自動検出など、最新のサイバー犯罪にも対応しており、**ウイルス定義ファイル**も頻繁に更新される。また、パソコンだけでなくモバイル機器へのインストールにも対応したソフトが多いので、スマートフォンなどの対策も万全だ(図1)。いざというときのウイルス駆除も強力で、中には駆除できない場合の返金保証をしているものまである。使用する機器の台数や必要な機能をよく考えて選択しよう。

Windows自体のセキュリティ対策で重要なのが、更新ファイルのインストールだ。WannaCryのようなウイルスの被害に遭わないためには、ソフトウエアの更新が欠かせない。Windows 10では自動的にWindows Updateが行われるが、以前のOSを利用しているなら、自動更新の設定をしておこう(図2)。

Chromeなど、Windows付属以外のWebブラウザーを使っている場

用語解説

ウイルス定義ファイル▼
セキュリティ対策ソフトがウイルスの検出で用いるデータファイル。新しく出現したウイルスに感染しないためには、定義ファイルを最新の状態にしておく必要がある。

●使わないプラグインは削除

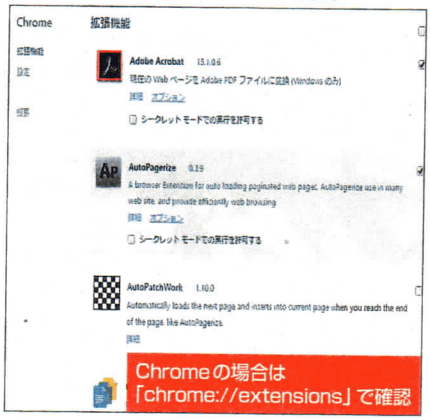


図3　Webブラウザーの拡張機能が勝手にインストールされる場合がある。定期的に確認して、使っていない拡張機能は削除しよう

●最後のとりで、システムイメージを作成

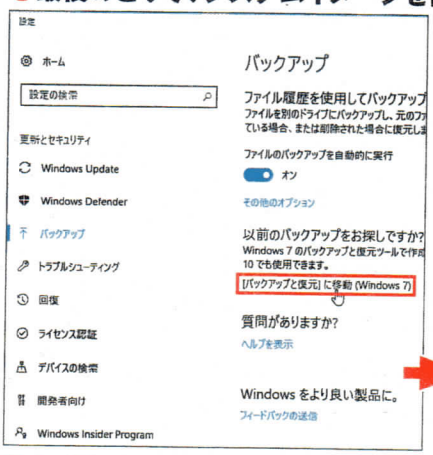


図4　Windows 10の場合、設定画面の「バックアップ」で「[バックアップと復元]に移動(Windows 7)」を選択

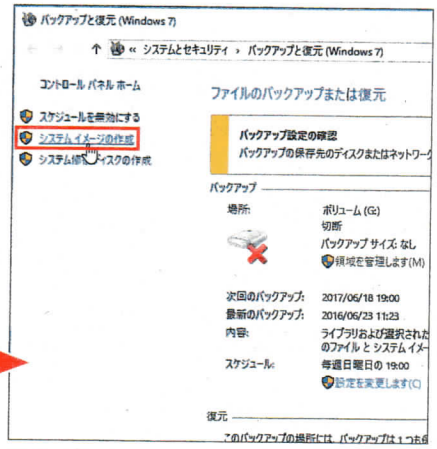


図5　「システムイメージの作成」を選択。表示される画面に従って、バックアップするディスクなどを選択していく

合は、適宜アップデートを行い、最新版に保つ必要がある。

万一に備える

いくら予防をしても、すり抜けてくるウイルスや、勝手に入ってしまう拡張機能、アプリなどもあるかもしれない。そうした侵入者を逃さないためには、定期的にウイルスチェックをかけたり、見知らぬアプリや拡張機能が入っていないか確認したりすることが大切だ(図3)。

マルウエアの中には、データやシステムを破壊するものもある。万一の場合に備えて、正常に動いている状態のストレージを丸ごとバックアップしておけば、最悪でもその状態までは戻せる(図4、図5)。

最新の犯罪手口に備えるには、セキュリティの最新情報を知っておくことが大切だ。図6に代表的なWebサイトをまとめたので、定期的にチェックしてほしい。そして、万一被害に遭ったときには、図7の相談窓口を利用して、被害を最小限に食い止めよう。

●セキュリティの最新情報はここでチェック

運営	名称	URL
警察庁	@police	http://www.npa.go.jp/cyberpolice/
情報処理推進機構(IPA)	情報セキュリティ	http://www.ipa.go.jp/security/
シマンテック	セキュリティレスポンス	http://www.symantec.com/ja/jp/security_response/
トレンドマイクロ	インターネット セキュリティ ナレッジ	http://www.is702.jp/
フィッシング対策協議会	フィッシングに関するニュース	https://www.antiphishing.jp/news/
ラック	注意喚起の記事	https://www.lac.co.jp/lacwatch/alert/

図6　セキュリティ関連の情報に気を付けるのも大事な防御策だ。これらのWebサイトで最新情報をチェックしよう

●万一のときは相談窓口へ

	運営・名称	連絡先
ウイルス、不正アクセス、サイバー攻撃	情報処理推進機構(IPA)	03-5978-7509 anshin@ipa.go.jp
	警察庁 サイバー犯罪相談窓口	https://www.npa.go.jp/cyber/soudan.htm
フィッシング被害	フィッシング対策協議会	https://www.antiphishing.jp/registration.html
違法な書き込み	違法・有害情報相談センター	https://www.ihaho.jp/
	セーファーインターネット協会	https://www.safe-line.jp/
迷惑メール	日本データ通信協会 迷惑メール相談センター	http://www.dekyo.or.jp/soudan/ihan/
詐欺サイト、通販詐欺などの被害	消費者庁 消費者ホットライン	http://www.caa.go.jp/region/shohisha-hotline.html

図7　万一サイバー犯罪の被害に遭ったり、相談したいことがあったりする場合は、相談内容に応じた連絡先に問い合わせてみよう