



サイバーセキュリティについて

自宅や職場においてインターネットやモバイル機器を安全に使用方法





目次

はじめに 3 ご挨拶: イアン・トンプソン フィデリティ・インターナショナル テクノロジー部長	パスワードのセキュリティ 14 - 18 安全なパスワードを作成して 管理できるツールやアイデアを ご紹介します
ソーシャルメディアの使用 4 - 7 ソーシャルメディアで公開する 情報や、その情報を誰に見られる のかを考えてみましょう	サイバー犯罪 19 - 26 通信手段の発達によって登場した 新たな犯罪を取り上げます
モバイルデータセキュリティ 8 - 10 モバイル機器や扱うデータの 安全性を確保する方法を ご紹介します	協力体制 27 - 30 会社の情報セキュリティへの 対応と、その重要性を ご説明します
子供の安全を守る 11 - 13 オンラインの世界に潜む 危険から子供を守りましょう	安全性の確保 31 - 33 デジタルセキュリティに関する 有益なヒントやテクニックを まとめてご紹介します



A handwritten signature in black ink, appearing to read 'Ian Thompson'.

イアン・トンプソン
フィデリティ・インターナショナル テクノロジー部長

サイバーセキュリティ について

サイバーセキュリティはフィデリティの業務において重要な位置を占めています¹。さまざまなサイバーセキュリティ対策を導入し、当社の情報や当社がお預りしているお客様の情報を確実に保護できるように取り組んでいます。本書では、サイバーセキュリティへの意識を高める必要性を詳しく説明し、簡単に効果的な手法について専門用語を使わずにご紹介します。

サイバーセキュリティは、職場だけではなく、日常生活においても重要です。現代のデジタル通信の世界では、自分の生活を家族や知人、同僚と一瞬にして共有することができます。そのおかげで生活は便利になりましたが、子供の教育の質、生活時間やコミュニケーション方法にも影響が現れています。

オンラインの世界にアクセスすれば多くのメリットを享受できるため、悪い点については忘れてしまいがちです。本書は自宅に持ち帰り、家族や友人と共有できるように作られています。自宅、外出先にかかわらず、サイバーセキュリティの実践的なガイドとしてお使いいただけると幸いです。●

¹www.fidelity.co.uk: Fidelityのセキュリティ対策とお客様自身でできるセキュリティ対策。



共有する情報に注意

ソーシャルメディアは、旧交を温めたり、新たな友達を作ったりできる、非常に楽しくて有益な手段です。興味のある物事を共有したり、最新のトレンドを把握したりもできます。残念ながら、Facebook、Twitter、YouTube、Pinterest、LinkedInなどのサイトは、犯罪者にも大人気です。その理由を知って驚かれるに違いありません。

31億7,000万人のインターネットユーザーのうち、ソーシャルメディアの利用者は**23億人**いるとされています。そして平均すれば**5.54個**のソーシャルメディアアカウントを所有しています。昨年だけでソーシャルメディア人口は**1億7,600万人**増えました。

出典：brandwatch.com

² Mashable.com：10人がソーシャルメディア上のミスで職を失った。

サイバーセキュリティについて

ソーシャルメディアの使用

ソーシャルメディアを使った経験があれば、夢中になってしまう理由をよくご存じのほうです。たとえば、自分の意見を投稿すると、瞬時に反応が得られます。また、自分が参加した会話がきっかけで、人々の生活が大きく変わるかもしれません。服装や食事に影響を与えたり、政府や政治さえも左右したりする可能性があります。

しかし、ご存じのとおり、ソーシャルメディアにはマイナスの面もあります。「共有し過ぎ」に関する逸話²を読んだことがあるかもしれません。たとえば、Facebookにアップした休暇中の不名誉な写真が検索で発覚し、採用試験に不合格となってしまった方もいます。

しかし、ソーシャルメディアを使用する上で本当に危険なのは、情報から利益を得ようとする犯罪者の存在です。犯罪者がどのような情報を探し、得た情報で何ができるのかをこれからご説明します。また、自分が意図している以上の情報を共有しないようにというお話もお伝えします。

ハッキングの内情

たとえば私がハッカーで、インターネット上のあなたのID情報を盗みたいとします。オンラインバンキングやウェブメールなど、インターネット上でサービス登録する際には、セキュリティ用に質問と答えを設定するように求められることがあります。たとえば「母親の旧姓」、「ペットの名前」、「誕生日」、「子供の頃のあだ名」などです。



ここで、ソーシャルメディアに載せている情報を考えてみましょう。私があなたのメールアドレスを知っていたら、これらの質問の答えを調べることができるでしょうか？ Facebookにペットの写真を投稿して、名前に言及していませんか？ 誰かがコメント欄にあなたのあだ名を書いていませんか？ あなたの誕生日は書かれていませんか？

情報は割と簡単に収集できるのです。

サイバーセキュリティについて

ソーシャルメディアの使用

全体で若い年代の**60%**がソーシャルメディア上で自身の写真を共有したことがあり、友人や家族の写真も多くの若者が共有しています。
若い年代の半数が自分の日常の様子を常時更新して、共有しています。

出典: statista.com

ソーシャルメディアでの調査を終えたら、あなたのウェブメールアドレスの「パスワードをお忘れの場合」のリンクをクリックします。そこから先程の調査で得た情報を使い、セキュリティ用の質問に答えます。

これであなたのメインのメールアドレスを乗っ取ったので、あなたが利用しているすべてのオンラインアカウントで「パスワードリセット」をクリックします（メールをすべて見ることができるため、あなたが登録しているサービスは把握できています）。私が乗っ取ったメールアドレスにパスワードリセットの要求が届くので、パスワードをすべて変更し、あなたから権限を取り上げることができます。

ハッカーがあなたの人生にどれほどの損害を与えられるか考えてみてください。ローン申請されるかもしれません。クレジットカードの申し込みは？ Amazonで何でも自由に購入されてしまったら？ それとも他人に絶対知られたくない秘密を盗み見られたら・・・。

共有する情報に注意

ソーシャルメディアを楽しみながら安全性も確保する第一歩は、「投稿する前に考える」ことです。オンラインアカウントを乗っ取るために使われる可能性のある情報については、よく考えてから投稿してください。具体的には、自宅の住所、メールアドレス、電話番号や誕生日といった情報です。セキュリティ用の質問の答えを設定するときは、パスワードと同じように考えてください。架空の情報、複雑なコードやフレーズを使って回答を設定します。

公私を分ける

人は誰しも個人的なものを共有したいと思うことがあります。どうしても共有する必要がある場合には、公開範囲をプライベートに設定するのが最善です。

ソーシャルメディアサイトのプライバシーとセキュリティの設定をチェックし、家族や友人だけがあなたのページを見られる設定になっているかを確認します。ぜひこのように設定してください³。

自分の居場所を伝えない

あなたの居場所をみんなに知らせることは、自宅にいないタイミングを知らせることであります。

窃盗犯があなたのTwitter（あるいはFoursquare、Google Buzzタイムラインなど）を見ていれば、盗みに入るのに最適な時間がわかります⁴。

利用しないアカウントを削除する

サイトを利用しないと決めたら、そのアカウントは削除してください。放置しておくとなんか不正使用される可能性があります。

よく考えてから情報を共有する

オンラインで共有した情報は、永久に残ります。共有しようとしているものが1年後（あるいは翌朝）、誰かに見られても問題ないのか、少しの間、考えてみてください。

ソーシャル
メディアでの
行動は
永久に
Googleに
残ります。

”

YourSocial.com

³ identity.utexas.edu: ソーシャルメディアのプライバシー設定の管理方法。



あなたの尊敬する人が投稿を読んでも大丈夫ですか？ その投稿が永久に消せない烙印のように残っても問題ありませんか？ いずれかに「いいえ」と答えるなら、「送信」ボタンを押さない方がいいかもしれません。

「友達」は誰かを知りましょう

たくさんの「友達」のリストを作ることはワクワクしますが、「友達」についてどの程度知っていますか？

実際、それだけの多種多様な人達を深く知ることは可能なのでしょうか。

家族と同じように信頼しているのであれば、すべてを共有しても構いません。しかし、たとえばその人たちに留守中の自宅に入られても大丈夫ですか？ もしそうでなければ、重要な情報を共有する際には慎重に考えてください。

怪しいと感じたら削除する

聞いたこともないようなサービスに登録するように依頼される、知らない人から友達リクエストが送られてくる、電子メールやTwitterにオンライン広告や正体不明のリンクが記載されている、といったことは、すべて個人情報を盗もうとするサイバー犯罪者の手口です。クリックする前に調べてみてください。あるいは、そのまま削除してください。●

⁴ Pleaserobme.com: 過度の共有に対する意識を高める。



外出中のデジタル セキュリティ

外出時にいつもモバイル機器、タブレット、スマートフォン、ノートPCを持ち歩いているならば、自宅にいるときと同様に厳重なデジタルセキュリティ対策を取る必要があります。これらの機器は紛失したり、置き忘れたりしやすいことに加えて、比較的安全な個人のWi-Fi環境ではなく、悪意に満ちた広大なサイバー世界の中で使用されます。

スマートフォンユーザーは世界中に**26億人**以上います。**87%**のスマートフォンユーザーが常にかたわらにスマートフォンを持っています。2016年に行われた調査では、PCからの検索よりモバイル機器を使用した**検索の方が多い**という結果が出ています。

出典: deviceatlas.com

サイバーセキュリティについて

モバイルデータセキュリティ

最近では、電子メール、財務資料、業務データ、企業資料、出張スケジュールなどの機密データをモバイル機器に保存する傾向が増えています。時間や場所を問わず、このようなデータにすぐにアクセスして編集できるからです。

クラウド上に保存されている情報にモバイル機器でアクセスする機会も増えています。Dropbox、Evernote、Microsoft OneDrive、Apple iCloudなどのデジタルストレージを使用しているならば、ポケットやバッグに個人データ一式を入れて歩き回っているのと同じです。

それに加えて、スマートフォンを（数ある用途の中でもとりわけ）クレジットカード、スマートキー、ヘルスマニターとして使用することが増えてきています。ハッカーがこの個人データの宝庫にアクセスする事態を阻止することが、いかに重要かわかりいただけるはずですよ。

モバイル機器はどこにでも持ち運べるため、置き忘れ、紛失、ハッキング、盗難の確率は非常に高くなります。こうしたことは、常時アクセスでき、便利であることの代償とも言えますが、適切な対策によってリスクを最小限に抑えられます。

内蔵機能を使う

あなたのデータを守る最も簡単で効果的な方法は、ちょっとした手間を惜しまず、自分の機器のセキュリティ設定を見直すことです。パスコードを使って画面をロックするだけで、本人以外の不正使用を未然に防ぐことができます⁵。

探してデータを消去する

Android、iOS、Windowsのモバイル機器には、遠隔で検出、ロック、消去する機能が標準装備されています。自分の機器をなくした場合に、すぐにこの機能を使えるように日頃から準備してください。

Wi-Fiに潜む危険

喫茶店、図書館あるいはその他の公共の場で無料のWi-Fiを使用するときは、接続前に必ずネットワーク名をスタッフに尋ねるか、店内表示で確認してください。Windows機器では、「セキュリティの種類」がWEPまたはWPA2になっていることを確認します。MacやiOSでは、Wi-Fi設定で錠前のシンボルを確認します⁶。インターネットの閲覧が終わったら、使用したサービスから必ずログアウトしてください。次に、そのWi-Fiネットワークを機器から消去してください。

バックアップを取る

家を出る前に、必ずデータと設定のバックアップを取るようしておけば、失うのはハードウェアだけで済みます⁷。

モバイルファイアウォールを利用する

ホテルのLANポートや公共のWi-Fiに接続できる「ポータブルルーター」を使用すれば、すぐに安全なホットスポットを構築できるため、同じネットワークに接続している悪意あるユーザーに対する防御を強化できます。多くの機種では、固有のパスワードを設定することで、さらに安全性を高められます。

⁵ Lifehacker.com: 暗号化でOS全体を他人の目から隠す。

⁶ Lifehacker.com: プライバシーを保護する最良のブラウザ拡張機能。

⁷ tabtimes.com: セキュリティ会社がモバイル機器の紛失と盗難による損害を公表。

スマートフォン盗難方法

IDG ResearchとLookout Mobile Securityでは、2014年にスマートフォンを盗難された2,403名を対象に調査を行いました。



53秒に1台のノートPCが盗難されています。
7,000万台のスマートフォンが毎年紛失し、持ち主に返るのはわずか7%です。

ノートPC紛失による損害額の80%はデータ漏えいが原因です。

出典：
channelpronetwork.com

大半のノートPCには、標準でソフトウェアファイアウォールがインストールされていますが、ウイルスまたはその他の悪意あるソフトウェアによって無効にされる可能性があります。ご自身のポータブルルーターを使用すれば、効率的にセキュリティを強化できます。

常に最新の状態に更新する

すべての機器を最新版にアップデートし、ソフトウェアを最新状態に保ってください。インストールされているアプリの自動更新機能がオンになっていることも確認します。

盗難防止のためロックする

モバイルPCをお持ちであれば、高品質なケーブルロックを買ってください。ケーブルロックは、モバイルPCに接続するスチール製のワイヤー

で、(壁のブラケットや金属製のポールのような)頑丈なものにかけてハードウェアを施錠します。時間をかければ切断することは可能ですが、窃盗犯の標的になる可能性は低くなります⁸。

コンピューターロックのメーカーであるKensingtonによれば、ノートPCの40%が個人用オフィスから盗まれています。職場にいるからといって、安全とは限りません。

何よりも重要なこと

自分のモバイル機器はいつも携帯するか、目の届く範囲に置くようにしてください。❶

⁸ consumerreports.org : スマートフォンの盗難被害が2013年には310万台に増加。

子供に安全な ネットサーフィンを

子供はコンピューターやインターネットが大好きです⁹。親が許可すれば、喜んで1日中インターネットを使っているでしょう。子供にはインターネットの「良い面」しか見えていないからです。ゲーム、ビデオ、動画、友達とのチャット、考えつく限りのあらゆる質問に対する回答、有名人の話題、音楽、Google Earthなど、さまざまな楽しみがあります。

8~11歳の5人に1人、
12~15歳の10人に7人が
ソーシャルメディアの
アカウントを持っています。
チャイルドライン支援セン
ターのウェブサイトには
320万件以上のアクセスが
あり、2013、2014年に
比べて**5%以上**増加して
います。

⁹Internetmatters.org:子供が
インターネットを安全に使用する
ための両親へのアドバイス。

出典: nspcc.org.uk

インターネットとともに育つ子供は、
オンラインで読むものはすべて
真実だと思っています。

”

Ofcom、
子供と親：
メディアと意識のレポート

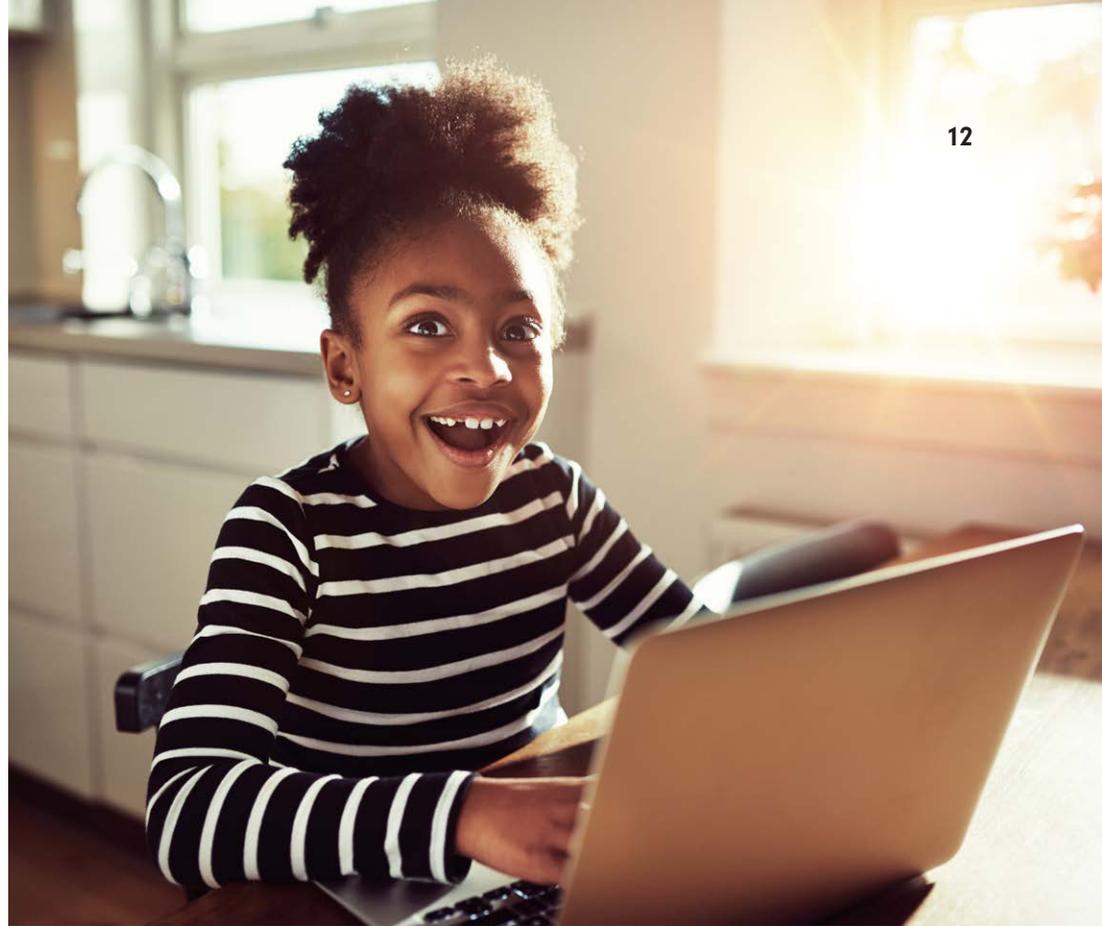
しかし、他のさまざまなことと同様に、知らないということが危険なのです。子供は、大人であれば知っているであろうパスワードセキュリティやネット荒らし、ネット上のマナー、フィッシング、サイバー犯罪、ハッキングなどについて知りません。

インターネットは、野放しで規制のない場であり、子供を守りたい親の考えとは相反する環境です。しかし、子供は、その世界に飛び込みたくてしょうがないのです。親はどのような対策から手を付ければいいのでしょうか？

環境をコントロールする

ネットサーフィン用のすべてのアプリには、安全性を高めるための設定が組み込まれています。まず、それについて知りましょう。強力な専用のセキュリティ対策ソフトウェアプログラムもあります。それによって、特定のサイトやプログラムへのアクセスに対して制限をかけたり、制限されているサイトを見ようとすると親に電子メールの通知を送ったり、打ち込まれた文字を記録したりもできます。

多くの子供には、そこまでの監視は必要ないはずですが、どのような対策が可能で、何が最適なのかを調べてみてください。ただし、100%の安全を実現できるシステムは存在しないことも忘れないでください。



子供とはいつも一緒に

子供が小さければ、絶対に1人でネットサーフィンをさせないでください。知らない街へ子供を連れていった際には、1日中自由に走り回らせたり、他人の家に出入りさせたりはしないはずですが、どれほど強力なセキュリティ設定を施していても、インターネット上に子供を1人で放置しないでください。

子供と正直に話す

多くの親は、自分の子供にいつまでも純真でいてほしいと願い、その反面では多少の自由は認めてあげたいと思っています。その微妙なバランスを実現するには、子供が巻き込まれる可能性のある危険について、包み隠さず誠実に話し合うことから始めましょう。



どの程度直接的に話すかはご両親次第で、当然、子供によっても異なります。しかし、少なくとも不適切なコンテンツや悪人の存在については、話し始めておくことが重要です¹⁰。子供を恐怖に陥れる必要はありませんが、友達や兄姉にそそのかされて愚かな行動をする前に、基本的な知識を教えておいてください。

小さな「セキュリティエージェント」を育てる

両親や兄姉が夢中になっていることに子供は興味を持つものです。したがって、好奇心旺盛な子供には、デジタルセキュリティへの興味を喚起させるのも手です。

次のシステムソフトウェアの更新時あるいはセキュリティパッチの適用時に親が付き添って、子供自身にそれをさせ、なぜ必要なのか、どのように役に立つのかを伝えてください。作業が無事終わったら、家族初の「デジタルセキュリティエージェント」になったことをお祝いしてあげてください（コードネームを付けてあげてもいいかもしれません）。

楽しみながら、一緒にオンラインでセキュリティの調査をしたり、厳重なパスワードの作り方を教えたりしましょう。同世代の子供よりも高度な知識を学んでいることを子供に伝えてください。また、その過程は親にとっても学習の機会となります。❶

¹⁰ Thinkuknow.co.uk: インターネット上の安全に関する知識を親子でテスト。

効果的なパスワードの設定

パスワードはデジタル世界への鍵となるもので、オンラインバンキングから電子メールに至るまで、すべてに必要です。面倒に感じる場合もありますが、個人情報を保護するには不可欠なものです。ここからは、適切で厳重なパスワードによってアカウントの安全性を保つ方法をご説明します。

70%の人はウェブサイトごとに固有のパスワードを使用していません。
全アカウントの98%で使用頻度が上位10,000例のパスワードが使われています。

出典：
passwordresearch.com

サイバーセキュリティについて パスワードのセキュリティ

2015年、米国内国歳入庁 (IRS) は多数のシステムのパスワードに「password」という言葉を使い続けていて大きなトラブルになりました。

出典: theguardian.com

パスワードは簡単で使いやすい、安価なセキュリティ手段です。日々の業務で使用するのみならず、電子メールやソーシャルメディアを通して友人や家族とやりとりする際にも使用される、標準的なセキュリティの管理方法です。

たとえば、対面で銀行の窓口業務を行っていた時代には、署名、写真付きの身分証明書、口座番号で本人確認する必要がありました。あるいは、カウンター奥の顔馴染みの行員に本人であることを確認してもらう必要がありました。しかし、インターネットの時代では、ユーザー名とパスワードの2つだけで本人確認が可能です。

そして、ユーザー名とパスワードという2要素での手続きが普及した結果、現在のシステムは非常に脆弱になったのです。すべてのアカウント、プロフィール、アプリ、ログインに複雑なパスワードが必要になっているために、「パスワードの悪夢」と呼ばれる状態になっています。

パスワード管理の要求は、率直に言って非現実的であり¹¹、多くの人がパスワード管理の基本ルールを破っています。複数のサイトでパスワードを使い回したり、できる限り簡単に短いパスワードを使用したりして、パスワードが覚えやすく、子供じみたものになってしまいます¹² (次ページの表を参照)。



パスワードのハッキング

ハッカーがパスワードを破る手口は多数ありますが¹³、それらの多くは簡単に入手可能なソフトウェアであり、特別なスキルがなくても使用できます。ユーザー自身でパスワードを脆弱なものにしている点も見逃してはいけません。

パスワードを破る方法

たとえば、お気に入りのオンラインショッピングサイトで「MySecure Password」というパスワードを使用しているとしましょう。ログインページで入力されたパスワードは、サイトのデータベースには直接

¹¹ teamsid.com: 2015年最悪のパスワードを発表。

¹² passwordmeter.com
password.kaspersky.com:
安全なパスワードチェックサイト。

¹³ security.blogoverflow.com:
パスワードをハッシュ化すべき理由。

サイバーセキュリティについて

パスワードのセキュリティ

2015年によく使われたパスワードのトップ10

SplashDataが毎年発表している第5回「最悪なパスワードリスト」からは、いまだに脆弱なパスワードが使われている状況がわかります。

順位	パスワード	前回の順位
1	123456	順位変わらず
2	password	順位変わらず
3	12345678	1ランクアップ
4	qwerty	1ランクアップ
5	12345	2ランクダウン
6	123456789	順位変わらず
7	football	3ランクアップ
8	1234	1ランクダウン
9	1234567	2ランクアップ
10	baseball	2ランクダウン

「MySecurePassword」としてではなく、「ハッシュ化」されて保存されます。

ハッシュ化とは、標準的なアルファベットと数字（プレーンテキスト）で構成されたパスワードを、ランダムで無意味な文字列（ハッシュ）に変換する方法です。ハッシュ化された「MySecurePassword」は、仮にですが、「Vxc5\$MnfsQ4iN\$ZMTppKN16y/tlsUYs/obHlhdP.Os80yXhTurpBMUba」という文字列になります。

ご覧のように、ハッシュ化された文字列は元のパスワードのように見えません。それでは、ハッカーにアカウントのハッシュを入手されても（入手は驚くほど簡単です）、個人情報や安全でしょうか？ 実は安全ではありません。ハッカーは、ハッシュコード文字列とフリーソフトウェアがあれば、パスワードのハッシュを分析して元の「MySecurePassword」

を知ることができます。国際的な犯罪団体のメンバーやスパイ組織の秘密エージェントである必要はありません。12歳の子供でも簡単にできます。具体的には次のような方法があります¹⁴。

辞書攻撃:何百万個もの標準的な単語、句、数字、有名な成句などを組み合わせたデータベースを、ハッシュ化ソフトウェアで実行します。あなたのパスワードのハッシュと一致する文字列が生成されるまで、1分間に何千回も繰り返します。「Vxc5\$MnfsQ4iN\$ZMTppKN16y/tlsUYs/obHlhdP.Os80yXhTurpBMUba」という文字列が生成されれば、該当するパスワードが「MySecurePassword」であるとわかります。辞書データベースを使用することで、このプロセスは大幅にスピードアップします。大半の人は名前、地名、動詞、形容詞、名詞などを使用してパスワードを作成するからです。

総当たり攻撃:辞書攻撃に似ていますが、既知の語句を使用して一致するパスワードのハッシュコードを見つける代わりに、ありとあらゆる文字、数字、特殊文字を使ってコードを解読しようとします。3桁の数字でロックするダイヤル錠を例に考えてみましょう。総当たり攻撃では、最初に1-2-3を試し、次に1-2-4を試すという具合に、あらゆる組み合わせを順番に試します。辞書攻撃より時間はかかりますが、非常に有効な手法です。

2010年1月

にTwitter社は非常に簡単な**370個のパスワード**の使用を禁止しました。以下は禁止されたパスワードの例です。
「000000」
「letmein」
「aaaaaaaa」
「whatever」
 そして**「stupid」**

出典: trendhunter.com

¹⁴ security.stackexchange.com : 辞書攻撃と総当たり攻撃の違いは？ 5つの基準。



セキュリティ用の質問を破る:多くの人は、パスワードを決める上で、家族の名前、ペットの名前、年齢、誕生日、好きな色／歌／スポーツ選手／有名人などを参考にしています。ソーシャルメディアにそのような情報を公開していると、アカウントをハッキングされる危険性があります¹⁵。詳しい手口や対策については、本書の「ソーシャルメディアの使用」セクションを参照してください¹⁶。

簡単なパスワードの使用:セキュリティ面で最悪なのは、使用頻度の高いパスワードの上位10例を使用することです（本項の最初のページを参照）。10文字未満で、大文字、特殊文字（*&^%\$£@など）、数字を使用

していないパスワードでは、セキュリティを危険にさらすことになります。複雑なパスワードに変更しないのは、まだ被害が発生していないから、というのが主な理由です。ほとんどの人は電子メールのアカウントがハッキングされても、そのパスワードを変えるだけで、それ以外を変更しません。深刻な被害が発生してから行動を起こすのでは、遅過ぎます。

パスワードの使い回し:電子メール、オンラインバンキング、ソーシャルメディア、ショッピングとそのたびに違うパスワードを作り、覚えるのは大変です。

¹⁵ slate.com : 新婚旅行で訪れた都市は？ およびその他の簡単な銀行のセキュリティ用の質問。

¹⁶ goodsecurityquestions.com : 適切なセキュリティ用の質問

ハッカーの種類

ブラックハットハッカーやホワイトハットハッカーという用語を聞いたことがあるかもしれませんが、その違いはご存じですか？ 違いは倫理に関わっています。



ホワイトハットハッカー

倫理的なコンピューターハッカーで、組織のセキュリティシステムのテストを専門としています。



ブラックハットハッカー

一般に認識されているハッカーです。広範な知識を持つ個人で、セキュリティを回避し、侵入・破壊を目的としています。



グレイハットハッカー

倫理規範が曖昧で、ハッキングスキルも優れていますが、悪意は持っていません。



ハクティビスト

政治やモラルに関する理由からハッキングを行います。多くの場合、フリースピーチ運動や人権運動に関係しています。

しかし、すべてに同じパスワードを使い回せば、1つがハッキングされるとすべてに被害が及ぶことを忘れてはなりません。すべてを1つのパスワードで済ませようとすると、すべてを失いかねないのです。

有効な対策とは？

100%の安全はありませんが、以下の10項目を実行すればセキュリティが破られる危険性を可能な限り低減できます¹⁷。

1. オンラインアカウントごとに異なったパスワードを使用する。

2. パスワードマネージャーの使用を検討する。パスワードマネージャーは、すべてのウェブサイトのパスワード情報を作成、記録、暗号化、保管してくれます。ウェブサイトへのログインを自動化する機能も備わっています。1つのマスターパスワードを覚えるだけで済み、それ以外のことはパスワードマネージャーに任せられます。
3. 定評のあるパスワード強度チェックサイトを使用して、選択したパスワードの強度をチェックする。
4. インターネットカフェや図書館など公共の場にあるコンピューターや共有のコンピューターには、自分のパスワードを入力しない。
5. 同様に、セキュリティが確保されていない公共のWi-Fiに接続している際は、自分のパスワードを入力しない¹⁸。
6. パスワードを定期的に変更する。同じパスワードを再利用したり、古いパスワードと類似したパスワードを設定したりしないでください（たとえば、*SecurePasswordApril*を*SecurePasswordMay*に変更することは避けず）。
7. 他人には絶対にパスワードを教えない。
8. 大文字、小文字、数字、特殊文字を組み合わせ、少なくとも10文字を使用する。数字と他の文字を混在させ、同じ文字をパスワードの先頭や末尾に並べないでください。可能な限り、各サイトで許容されている最大文字数を使用します。文字数が多いほど、好ましいパスワードです。
9. ログインした機器を放置したまま離席しない。
10. パスワード入力時には、誰かに見られていないことを確認する。①

6文字の小文字だけで構成されているパスワードは、わずか**10分**で破られます。2文字追加し、大文字をいくつか使用するだけで、所要時間は**3年**に急増します。さらに1文字加え、数字と記号をいくつか使用すると、破るのに**4万4,530年**もかかります。

出典：
Stopthehacker.com

¹⁷ passwordday.org: パスワード作成上のアドバイスと情報。

¹⁸ usa.kaspersky.com: 公共のWi-Fiネットワークには多くのセキュリティリスクがありますが、オンラインでの安全性とセキュリティを確保できる方法も多数存在します。



意識を高めて セキュリティを確保

組織的な犯罪から、秘密裏の監視、外国政府機関によるハッキングまで、違法行為は常に存在しており、通信やデータ保管に脆弱性があれば攻撃を受けかねません。ほとんどの人は問題なくインターネットを使用していますが、基本的なセキュリティ上の注意を怠れば、誰もがサイバー犯罪の犠牲になる可能性があります。

アメリカでは、2014年に約**3,180万人**の消費者がクレジットカードを不正利用されました。2013年の3倍以上の人数です。イギリスでは、2015年の第1四半期に、なりすまし詐欺が前年より**27%**増えました。現在では、報告された全詐欺犯罪の**ほぼ半分**を占めるに至っています。

出典: nasdaq.com

ボットネットとスパイウェアの違いをご存じですか？

最も頻繁に発生する不正コンピューター侵入や悪用について、以下で説明します。

サイバー犯罪用語

ボットネット (Botnet)

コンピューターをウイルスに感染させ、遠隔操作できる「奴隷」(ゾンビとも呼びます)に変えます。犯罪組織は、犯罪の実行手段としてそのコンピューターを利用します。

ファームング (Pharming)

正規のURLからリダイレクトして、偽のウェブサイトへ誘導します。

フィッシング (Phishing)

あたかも正規の会社のメールやテキストメッセージ、ウェブサイトに見せかけて、個人情報(パスワードなど)を収集したり、あなたにリンクを開かせてシステムをウイルスに感染させたりします。

ランサムウェア (Ransomware)

マルウェアの一種で、コンピューターの全データを暗号化します。次に、ファイルを復元するための金銭の支払いを要求するメッセージを表示します。

スパイウェア (Spyware)

本人の知らない間に個人情報(パスワード、閲覧履歴など)を収集します。インターネットからファイルをダウンロードするときに、本人の承諾なく、あるいは本人の知らない間にインストールされる場合が大半です。

トロイの木馬 (Trojan horse)

悪意のあるソフトウェアで、正規の(あるいは正規に見える)プログラムを装ったり、それに潜り込んだりします。

一見無害に見える行為(メールアプリの使用、インターネットの検索、ファイルのダウンロード、ゲームのプレイ、新たなウェブサイトやサービスへのサインアップなど)でも、コンピューターやモバイル機器がウイルスやスパイウェアに感染し、データの損失、個人情報の窃盗、あるいは深刻な詐欺につながる可能性があります。

このような攻撃に対する最良の防衛策は、サイバー犯罪者がコンピューターへの侵入に使うさまざまな策略やテクニックを可能な限り知っておくことです¹⁹。あなたに隙がなければ、サイバー犯罪者は侵入できないからです。

左の一覧記事をご覧ください。一部はご存じかもしれませんが、一般的なサイバー犯罪の用語を説明してあります。

以下のページでは、犯罪者の手口や被害を防ぐ方法を詳細に解説します。

フィッシング

フィッシングでは通常、電子メールが利用されます。金銭を得たり、悪意のある活動を行ったりするために、個人情報の収集やコンピューターへの侵入を試みます。多くの場合、フィッシングメールには偽サイトへのリンクが記載されているか、マルウェアを含んだファイルが添付されています。リンクをクリックしたり、ファイルをダウンロードしたりすると、悪意のあるプログラムが起動します。

2015年には、銀行口座へのオンラインアクセスで金銭を詐取しようとするマルウェアについて、感染の試みの報告が**196万6,324**件にのぼりました。

出典: securelist.com

¹⁹ getsafeonline.org: 自分自身とコンピューターの保護。



世界中の疑うことを知らない人々に、何百万通ものフィッシングメールが毎日送りつけられ、被害が発生しています。中にはすぐに詐欺だとわかるメールもありますが、非常に巧妙なメールもあります。本物のメールと詐欺メールをどのようにしたら区別できるのでしょうか？ フィッシングメールの可能性があると判断する方法を6つ、以下にまとめました。

1 メールに怪しいURLや内容に合わないURLが記載されている

怪しいと思ったときは、埋め込まれているURLの整合性をチェックします。フィッシングメールのURLは有効なURLに見えますが、その上にマウスのカーソルをかざすと、実際のハイパーリンクアドレスを確認でき

ます。実際のハイパーリンクアドレスと表示されているアドレスが異なっていれば、詐欺メールの可能性が高いと判断できます。

2 メールにスペルミスや文法のミスがある

大手企業がメールを送信するときは、スペルや文法のチェックを行い、法務部門の検査を受けるのが普通です。スペルミスだらけならば、大手企業の法務部門のチェックを経たメールではない可能性が高いと言えます。

3 個人情報（特にパスワード）を要求する

普通の企業は、メールを通してパスワードやログイン情報の送信または

確認を要求することはありません。企業側はすでにその情報を知っているはずですし、あなたが誰かを確認する方法は他にいくつでもあります。つまり詐欺メールの可能性が高いのです。

4 顧客に合わせた挨拶や情報の記載がない

銀行やクレジットカード会社など、セキュリティを重視している企業からの正式なメールであれば、挨拶内にアカウント番号の一部やユーザー名が記載されているのが一般的です。単なる「ユーザー様」のような挨拶には注意する必要があります。

5 緊急性を強調している

今すぐ行動しないと損害が発生する、アクセスが停止される、などの文面はあなたに考える余裕を与えないことが目的です。時間をかけて、じっくり調査し、ハイパーリンクを再確認してください。また、他の手段（直接電話する、訪問する、手動でURLを入力してウェブページを開くなど）を使って送信者に連絡を取ります。

6 何かが「おかしい」

本来のロゴと少し違う、メールの文章が奇妙だ、と思う感覚が重要です。詐欺に対する最良の防衛策は、常識的判断力です。

怪しいと思ったら、破棄してください。

メール、リンク、添付ファイルの正当性に少しでも疑問を感じたら、それを削除するのが一番です。開封したり、転送したり、後で人に見せるために保存したりしないでください。後悔先に立たずです。

フィッシングは、犯罪者がコンピューターをウイルスに感染させたり、個人データを盗んだりする際に最もよく使われる手口です。フィッシングに成功したら、犯罪者は次に何をしようか？次に説明するランサムウェア攻撃かもしれません。

デジタルハイジャック

ランサムウェア²⁰は、ハッカーが金銭を巻き上げる目的でよく使うようになった手法です。いわばデジタルを駆使した恐喝で、2種類あります。

画面をロックするランサムウェア

金銭の支払いを要求する画像によって画面がロックされ、支払い方法の詳細が表示されます。

暗号化ランサムウェア

システムのハードドライブ（ネットワークドライブ、外部ハードドライブ、USBドライブ、クラウドストレージを含む）に保存されているすべてのファイルが暗号化され、開けなくなります。犯人はファイルを復旧させるための金銭を要求してきます。

²⁰ blog.trendmicro.com :
ランサムウェアは2016年最大の脅威の1つ。

サイバーセキュリティについて

サイバー犯罪

ソーシャルメディア上でのフィッシング

Barracuda Networksが20カ国のユーザーを対象に実施した調査では、ソーシャルメディアの使用中に経験したセキュリティ被害やプライバシーの問題が明らかにされています。



ランサムウェアウイルスによっては、法執行機関からのメッセージを装い、違法なオンライン活動が検出されたので、逮捕されたくなければ罰金を支払うように要求してくることもあります。

対処方法

要求された金額を支払っても、ファイルが復旧できる保証はありません。犯罪者が約束を守らないからといって、誰かに文句を言うことはできません。最近増えているのは、接触してきた人物がプロの犯罪集団

からランサムウェアウイルスを買っただけで、被害者が支払いに応じたとしても、犯人は復旧方法さえ知らないという事例です。

法的な脅迫は単なる脅しで、犯人は法執行機関の人間ではないため、法的な効力はありません。また、警察もこのような形で接触してくることはありません。

データは元に戻らない可能性もありますが、信頼のできるコンピューターの専門家に助言を求めてみる価値はあります。コンピューターの修理やデータの復旧について相談してみてください。

最も重要な個人ファイルを確実に保護するには、外付けドライブにバックアップを取っておくことです。

あなたもゾンビ軍団の一員に？

遠隔操作プログラム(ボット)に感染したインターネット接続コンピューター群が、ボットネットを形成します²¹。

ボットネットは被害者に気付かれにくいハッキング手段で、感染した個々のPCは「ゾンビ」と呼ばれます。1人の司令官のもとで軍団を構成し、ボットに感染したコンピューター同士が連携します。あなたも知らないうちにゾンビになっている可能性があります。

75万3,684台のコンピューターからランサムウェアプログラムが検出され、**17万9,209台**のコンピューターが暗号化ランサムウェアの標的になっていました。

出典: securelist.com

²¹ welivesecurity.com: 最も恐ろしいゾンビボットネットのトップ5。

コンピューターが被害を受けたかどうかを知る方法

人間と同様に、コンピューターも具合が悪くなると、動きがおかしくなります。本格的な検査が必要かどうかを判断するには、以下のリストを参考にしてください。

感染チェックリスト

以下のチェックリストを参考にして、問題の有無を判断できます。1つ、複数、あるいはすべてに該当する可能性もあります。

- ✓ 予期しないポップアップが表示される（スパイウェアに感染している兆候）
- ✓ プログラムが勝手に起動するようになる
- ✓ セキュリティソフトウェアが動作を停止した
- ✓ コンピューターの起動にいつもより時間がかかる。勝手に再起動することがある。または、まったく起動しない
- ✓ コンピューター画面の表示が歪んで見える
- ✓ プログラムの起動に時間がかかる
- ✓ ファイルやデータが消えた、あるいは移動した
- ✓ システムソフトウェアが頻繁にクラッシュする
- ✓ ホームページがいつの間にか変わっている
- ✓ いきなりメモリ不足に陥った
- ✓ ファイルやデータの名前が変更されている
- ✓ インターネットサーフィンやウェブページの読み込みが遅くなった

PCが感染していると思ったら、セキュリティソフトウェアを更新し、フルチェックを実行してください。原因を見つけられない場合や対処方法がわからない場合は、信頼できる専門家に相談してください。

ボットネットを形成したハッカーは、コンピューター群からウェブサイトには大量の要求を繰り返し送りつけ、サイトをアクセス不能な状態に追い込みます（分散型サービス拒否攻撃（DDoS）と呼ばれます）。このような攻撃は、企業を脅迫し、金銭を要求するのに使われます。

ゾンビ軍団の司令官は、感染したネットワークを利用して、何百万通ものスパムメールを送信し、ウイルスやマルウェアを拡散させることもできます。これらはすべて、あなたのコンピューターを踏み台にしているかもしれません²²。

対処方法

システムがハイジャックされて、攻撃に利用されるリスクを減らす方法について、以下で説明します。

ファイアウォール

ファイアウォールを設置して、コンピューターに出入りする通信の監視と制御を行います。攻撃が検出されると、自動的に警告を発するように設定することもできます。

電子メールフィルターの使用

メールフィルターをかけることで、メールアプリに入ってくる迷惑メールの量と種類を制限できます。

最悪のボットネット国トップ5

2016年9月現在

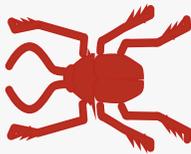
- 1 インド: 232万6,660台
- 2 ベトナム: 100万9,151台
- 3 中国: 79万6,087台
- 4 イラン: 65万1,753台
- 5 パキスタン: 45万8,816台

出典: spamhaus.org

²² uk.norton.com/botnet: ボットとボットネット — 増大する脅威。

被害の大きい3つの手口

ウイルス、ワーム、馬という実際の生物になぞらえることによって、これらは生き物のように行動するため無視しては危険であることを強調しようとしています。



コンピューターウイルス

悪意のあるコンピュータープログラムで、多くの場合、電子メールに添付されます。または、ユーザーにダウンロードさせて、コンピューターに感染します。ウイルスは、犯罪者があなたのコンピューターにアクセスできるようにしたり、パスワードなどの個人情報の収集、ウェブブラウザの乗っ取り、セキュリティの無効化などを行ったりします。



トロイの木馬

トロイの木馬は、正規のソフトウェアを装った、またはその内部に隠れた実行ファイルです。自分自身をインストールし、自動的に実行します。インストールされたトロイの木馬は、ファイルの削除やコピーを行ったり、ウェブカメラであなたを監視したり、キーボードに打ち込まれたすべての文字を記録したりできます。



ワーム

ワームはファイルやプログラムには寄生せず、単独で動作します。コンピューターのメモリに潜み、ネットワーク内やインターネット上の他のコンピューターに自分自身を送信します。信じられない程の増殖力は、個人のみならず、インターネットそのものにとっても脅威となります。

監視を怠らない

インターネットへの接続が遅いと気付いたら、システムツールを使用して、モデムが処理している通信量をチェックしてください。

何もダウンロード／アップロードしていないのに通信量が非常に多ければ、ボットネットの一部になっている可能性があります²³。

テクニカルサポートのなりすましに注意

詐欺師の中には、インターネットサービスプロバイダーのテクニカルサポート部門になりすます者さえいます。「不正なファイルやソフトウェアを見つけたので、あなたのコンピューターにリモートアクセスして除去する必要がある」などと連絡してきます。ご自分からインターネットサービスプロバイダーやコンピューターメーカーのヘルプデスクに問い合わせをしていなければ、そのような申し出は詐欺だと判断すべきです。

詐欺の仕組み

ハッカーは、インターネットプロトコル (IP) アドレスからインターネットサービスプロバイダーを特定できます。あなたにブロードバンド接続を提供しているプロバイダーがわかれば、そのテクニカルサポートになりすますのは簡単です。

サポート担当者の振りをした詐欺師はチャットや電話で連絡してきて、「システム内の感染ファイルを除去するには、あなたのパソコンをコントロールする必要がある」と説得にかかるでしょう。詐欺師にアクセスを許可してしまうと、感染したと称するファイルを除去するために金銭を支払うように要求してきます。

対処方法

自分から依頼した相手でなければ、決してコンピューターへのリモートアクセスをさせてはいけません²⁴。

最近5年間で、**2,700万人**以上のアメリカ人が個人情報を盗まれています。昨年1年間だけで、その内の**900万人**が被害にあっています。

出典：
stopthehacker.com

²³ f-secure.com: ボットネット クイックガイド - 正体、仕組み、被害。

²⁴ moneysavingexpert: 詐欺を止める30の方法。

サイバーセキュリティについて

サイバー犯罪

クラミング (Cramming)とは、顧客が注文も希望もしていないサービスの料金が、電話料金の請求書に追加される詐欺的行為です。また、消費者に対して適切に開示されていない通話料金やサービス料金が追加される場合もあります。

出典: en.wikipedia.org

そのようなテクニカルサポートのチャット画面が表示されたら、無視して閉じてください。また、同様の電話がかかってきたら切ってください。お使いのインターネットサービスプロバイダーに直接連絡し、事情を説明します。その際は、普段使用している番号または過去に使用したことのある番号に電話してください。

リモートアクセスを許した後なら、あなたのシステムはおそらく侵入されています。そのような場合は、機器をネットワークから切り離して、オペレーティングシステムを再インストールするか、信頼できるコンピューターサポートサービス業者に持ち込んで復旧してもらいます。データの完全なバックアップが取ってあれば、作業が非常に楽になります。

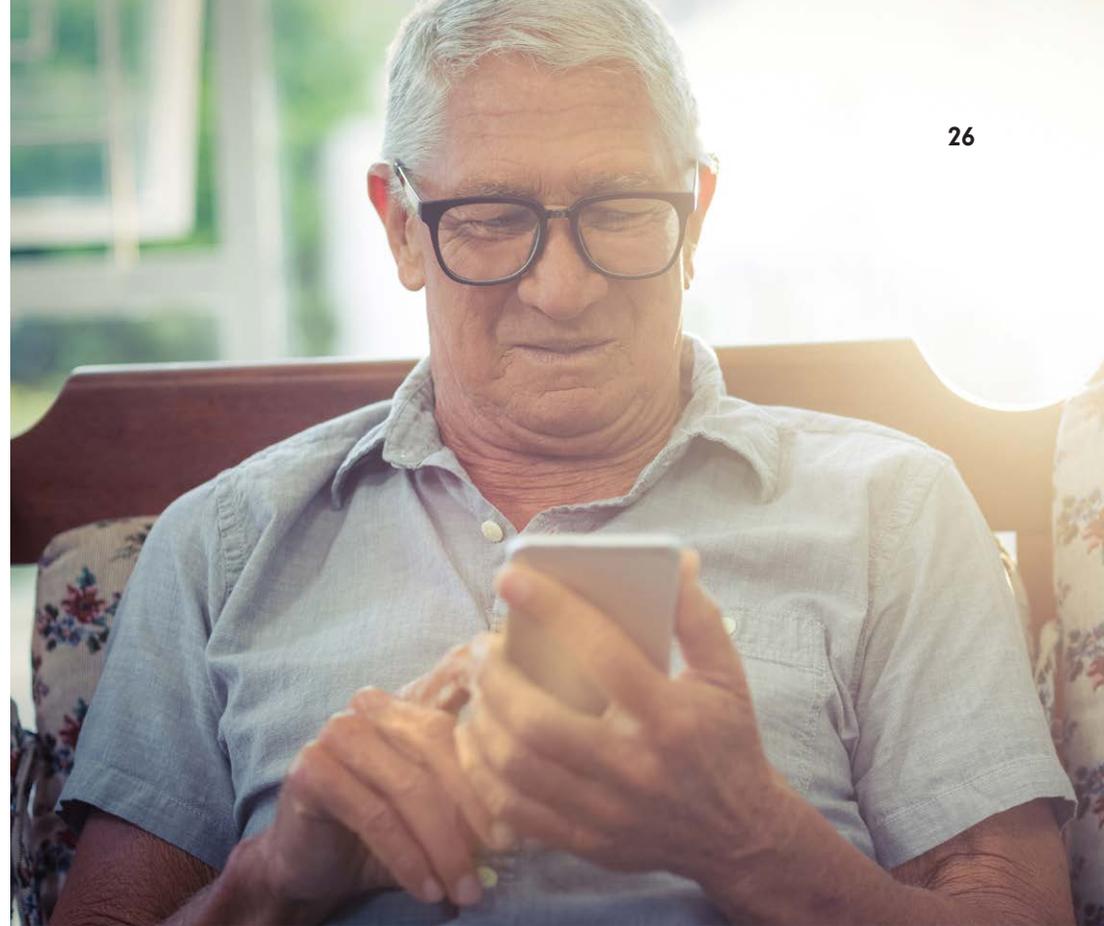
詐欺師からの電話

犯罪者は、あなたのセキュリティ情報を知ろうと21世紀の最新技術を駆使していますが、電話も相変わらずよく利用されます²⁵。

ヴィッシング (Voice-phishing) 詐欺では、たとえば銀行を装って、口座の不審な動きを警告してきます。または、ケーブルテレビ会社や警察の振りをして、あなたがクレジットカード詐欺の被害にあったと警告します。これらはすべて、あなたの口座情報やパスワード情報を詐取る目的です。

特に警戒が必要な状況

あなたのカードが不正に使われた、と電話がかかってきます。電話をかけてきた犯人は、あなたに正当な電話であることを確かめてもらうために、電話を切ってかけ直してほしいと言います。しかし、犯人の側



では、受話器を置かずにいることで、あなたの電話をつないだままにできます。これにより、あなたは自分がダイヤルした不正利用の対応窓口につながったと錯覚してしまいます。次に、誰かがあなたに対して、新しい口座に送金するように伝えてきます。しかし、あなた名義の口座だと言われても信じてはいけません。

対処方法

プレッシャーに負けて、気が進まない行為をしないでください。何かおかしいと思ったら、まず立ち止まって、考える時間を取ります。電話を切る勇気を持つことが大事です。礼儀を失わず、かつ毅然と電話を切りましょう。❶

²⁵ bbc.co.uk: 記録に残された詐欺: 電話詐欺師による1万2,000ポンドの詐取事件。

協力体制

企業経営者は、増大し続けるデータを収集、保管、活用するために、情報システムへの依存を強めています。経営者は、どのような種類のデータを収集し、どのように保管しているのかを従業員に公開する責任を負っています。一方、従業員側もデータの安全性をどうすれば維持できるかについて、自問自答しなければなりません。

Shred-it/Ipsos Reid
Information Security
Trackerによれば、回答者の
47%がコンソールには
施錠し、シュレッディング
サービス業者に機密文書を
シュレッディング処理させて
います。しかし、**46%**は、
情報の安全な破棄に関して
直接の責任者はいないと
答えています。

出典:shredit.com

サイバーセキュリティについて 協力体制

2015年に金融機関で検知されたセキュリティインシデントの41%は、信頼されてアクセスを許可された外部企業が原因でした。製造業でのセキュリティインシデントの62%には、従業員や元従業員が関与していました。

出典: pwc.com

私達の誰もが、物理的にもデジタル的にも、安全かつセキュリティの整った環境で仕事をする権利を持っています。そのような環境を作るには、現地政府のガイドラインや部署のポリシーに準拠するだけでなく、意識の問題も重要です。

リスクとのバランス

人がいる場所にはリスクが存在するのが現実ですが、リスクと自由の間でバランスを取る必要があります。

データを安全に保管できないような企業は、取引相手としては不適当です。しかし、セキュリティのプロセスが業務の妨げになっては元も子もありません²⁶。どんな状況にも円滑に対応できるようにすることが欠かせません。何事もバランスです。データや顧客、企業を守る方法について、以下で説明します。

パスワード

どのような場合でも、仕事用のパスワードは誰にも教えないでください。付箋にメモしてPCの前に貼っておくのも当然してはいけません。詳細は、本書の「パスワード」セクションをご覧ください。

電子メール

電子メールについては、誰もが同じ間違いをした経験があると思います。簡単なミスにもかかわらず、今でも多くの人が間違い続けています。メールを送信する前には、宛先が正しいかどうかをしっかりと確実に確認しましょう。



機密情報の誤送信は、自分が恥をかき、会社も危機にさらす行為として、最上位にランキングされるものです。「送信」ボタンを押す前に、メールを暗号化する必要があるかどうかを検討し、宛先を再確認してください。

また、仕事のメールアドレスを仕事以外に使用しないでください。受信トレイがスパムメールだらけになって、フィッシング攻撃の被害を受ける可能性が高まります(本書の「サイバー犯罪」セクションを参照)。

²⁶ inspire-success.com:
職場のITセキュリティに関する
12の重要アドバイス

仮想世界、物理的なセキュリティ

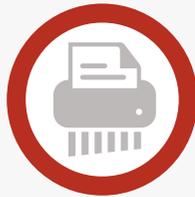
業務データを犯罪者の手から守るには、仮想世界での高度なセキュリティ手法だけでなく、現実世界における対策も講じる必要があります²⁶。

現実世界におけるセキュリティ



不審なものを見かけたら報告する

あなたの会社が入館許可証システムを導入していたり、IDバッジを発行していたりすれば、セキュリティ部門が存在しているはずですが、バッジを着用していない人や、通常とは違うものを見かけたら、必ず報告するようにしましょう。自分で直接対処する必要はなく、気掛かりな点をセキュリティ部門に伝えるだけで構いません。犯罪者は、私達が戻込みして何も言わないだろうとタカをくくっています。



整理整頓

印刷した文書についても、デジタルデータと同じようにセキュリティに注意してください。離席するときは、デスク上に機密文書を放置しないようにします。1日の業務を終えた後は、鍵のかかる引き出しなどにしまい、コピー機やプリンターにも機密文書を一切放置しないでください。印刷した文書が不要になっても、そのまま捨てずに、シュレッダーにかけてください。



情報をむやみに教えない

電話でも電子メールでも、個人情報や機密情報は知らない人に教えないでください。その前に人物や会社の確認を行い、情報を知りたがっている理由を把握します。また、公共の場やインターネット上で業務に関する機密情報に言及しないようにしてください。どこで誰が聞き耳を立てているかわかりません。

画面のロック

離席するときは、自分のコンピューターをスリープモードにするか、画面をロックしてください。そうすれば、誰かがあなたの作業内容を見たいと思っても、パスワードが必要になります（ただし、パスワードを記載した付箋をキーボードの裏に貼り付けていたりすれば、意味がありません）。

仕事の自宅への持ち帰り

仕事上のファイルを自宅に持ち帰ることについて、会社の規定を確認してください。持ち帰りが許可されていれば、持ち運ぶ前にデータを暗号化するか、パスワードで保護されたドライブに入れることで、紛失した場合にも情報を保護できます。

機器の紛失や盗難の報告

仕事関連のデータが保存されている機器を紛失したら、できるだけ早急に関連部署に報告してください。紛失を報告するのは気が引けますが、機密情報が悪人の手に渡り、会社の対策ができていなければ、はるかに深刻な事態になってしまいます。

クリックする前に考える

インターネットから仕事用コンピューターにデータをダウンロードするときは、くれぐれも注意してください。特に「実行形式」(.exe) ファイルには警戒が必要です。本物のファイルか、あるいは業務システムに感染するウイルスが潜んでいるファイルかどうかは、ほぼ判別不可能です。



情報セキュリティ部門との連携

自社にIT部門や情報セキュリティ部門があれば、訪ねてみてください。どのようなデータセキュリティ対策を講じているか、自分が貢献できることは何かを質問してください。問題が発生した場合に誰に連絡すればよいかを把握しておけば、心の準備もできます。忘れないでいただきたいのは、情報セキュリティ部門はあなたの手助けをするためにいる、ということです。本書の執筆者もその一員です。

情報セキュリティ部門を面倒な人達と思うかもしれませんが、考えてみてください。情報セキュリティ部門は、これまでにない新たな環境で新たな脅威と向き合っているのです。

私達は、インターネットが持つ危険性と可能性に対応する必要がある、歴史上初の社会で生きています。誰にとっても初めての状況です。それがもたらす変化を心地よいと感じる人もいれば、そうでない人もいます。

しかし、結局のところ、現在はデジタル時代です²⁷。かつては、退社時に窓を施錠して夜間警報装置をオンにするだけで十分でしたが、現在は盗難対象が金銭や機器だけとは限らなくなっています。業務データを盗難されれば、顧客や信用など、すべてを失う時代となりました。21世紀の職場にふさわしいセキュリティ対策が必要です。❶

²⁷ cio.com : 誰もが情報セキュリティに関わる時代

少しの心掛けが重要

インターネットは西部劇の荒くれた時代とは違います。怪物のすむ森もなく、橋の下に巨人がいるわけでもないし、峡谷の盗賊もいません。本書で紹介してきたのは特に深刻な事例ですので、ここで本書を閉じてしまって、もう二度とインターネットは使わない、などと言わずに少しでもセキュリティ対策を見直してみてください。時間を割くだけの価値は確実にあります。

2015年の第1四半期（1～3月）には、イギリスの**成人の86%（4,470万人）**が直近3か月間にインターネットを使用しています（最近の使用者）。2014年第1四半期（1～3月）の推定85%から1ポイントの増加です。**成人の11%（590万人）**はインターネットの使用経験がありませんが、2014年第1四半期（1～3月）と比較すると1ポイント減少しています。

出典: ons.gov.uk

サイバーセキュリティについて

安全性の確保

理にかなった手順を踏むことで、サイバー犯罪や個人情報窃盗の被害にあう可能性を大幅に減らせます²⁶。多くの犯罪者は、最小限の労力で最大限の利益を得る方法を模索しています。玄関のドアや窓を開けたまま外出する人は、しっかりと施錠して外出する人に比べて、盗難にあう可能性はるかに高くなります。コンピューターやアカウントについても同様で、複数のセキュリティ手順で保護すれば、無防備なものに比べて、ハッカーなどの標的にされる確率を大幅に低くできます。ハッカーからの攻撃を受けやすい状態にしないことが重要です。

機器の保護

オペレーティングシステム、アプリ、ウェブブラウザを最新版にしておくことは、最も簡単で効果的なセキュリティ対策です。

自動更新機能を有効にして、最新のオペレーティングシステムやセキュリティパッチを取得してください。

データの保護

入念に考えられたパスワードを使用して、アカウントごとに別のパスワードを設定します。詳細は、本書の「パスワードのセキュリティ」セクションを参照してください。

セキュリティが確保された回線を使用して情報を送信してください。クレジットカード情報などの機密情報を送信するときは、アドレスバーに <https://> または **錠前アイコン** が表示されていることを確認します。公共の場にあるコンピューターや共有のコンピューターを使用して、パスワード保護されたアカウントやサイトにアクセスする必要がある場合

は、利用が終わったら必ずサインアウトしてブラウザウィンドウを閉じます。

何らかのセキュリティソフトをインストールしておいてください。アンチウイルス/マルウェア機能とファイアウォールを装備したものを推奨します。

共有し過ぎに注意

ソーシャルメディアの利用方法について検討してください。プライバシーとセキュリティの設定を行い、自分が投稿した情報を利用して犯罪者が何をできるか考えてみてください。詳細は、「ソーシャルメディアの使用」のページを参照してください。

フィッシング対策

フィッシングにはくれぐれも注意してください。電子メールやTwitterに記載されたリンク、偽ウェブサイト、魅力的過ぎる提案は、ハッカーが個人情報を詐取る常套手段です。警戒心を持って、おかしいと思ったら迷わず削除してください。詳細は、「サイバー犯罪」セクションを参照してください。

バックアップ

面倒かもしれませんが、何ものにも代え難い写真や、作業ファイル、その他のデジタル情報は、定期的に取り外し可能なドライブにバックアップを取ってください。ハードドライブやクラウドアカウントに問題が発生してもデータを保護できます。

²⁶ staysafeonline.org: 全米サイバーセキュリティ連盟が安全性確保のためのヒントとコツを公開。

仮想世界の概要

2015年1月時点で、世界人口のほぼ42%がインターネットにアクセスしています。2015年の世界におけるデジタル技術の利用状況をWearesocial.netが公開しました。



事前の準備

最悪の事態が発生したときの準備をしてください。あなたの個人情報やアカウントのセキュリティが侵害された場合に備えて、友人や取引先の電子メールアドレス、電話番号、住所を紙に書き写しておきます。クレジットカードの利用停止や銀行口座の凍結を依頼する電話番号を確認します。また、詐欺対策の法執行機関の名称や電話番号も調べておきます。このような対策により、犯罪者があなたの金融資産に自由にアクセスできる時間を最小限に抑えられます。

実行前に考える

今回限り、期間限定、特別価格などの謳い文句に私達は弱いものです。詐欺師はそこにつけ込みます。このような魅力的過ぎる話は、多くの場合、裏に悪意が隠されています。悪意を見破れるようになります。詐欺被害の実例や詐欺を見破った方法について読んでみてください。

無料旅行やiPadのプレゼントには誰でも魅力を感じますが、オンラインフォームに記入するだけで手に入るということはありません。それらは詐欺です。

まとめ

オンラインの世界はデジタルですが、現実のものではない、というわけではありません²⁷。インターネットを構成しているのは、現実の生活を送り、感情も持っている人々です。

大衆と一緒に流されるのは簡単で、刺激的かもしれませんが、インターネット上で起きる物事は重大であり、当事者に長期にわたって大きな影響を及ぼす可能性があります。自分がそうしてもらいたいように、他人に接しましょう。思いやりを持ち、意識を高めて、セキュリティも確保してください。本書をお読みくださり、ありがとうございました。📌

²⁷ youtube.com: インターネットの仕組み



最後までお読みいただきありがとうございました。

© FIL Limited 2017.

当資料は信頼できる情報をもとにフィデリティ証券が作成ないし編集しておりますが、正確性・完全性について当社が責任を負うものではありません。

当資料の情報は、2017年4月末時点のものであり、市場の環境やその他の状況によって予告なく変更する場合があります。

また、当資料は情報提供を目的としたものであり、個別の商品の推奨または勧誘を目的としたものではありません。

著作権等の知的所有権その他一切の権利はフィデリティ・グループに帰属し、許可なく複製、転載、引用することは固くお断りします。

(商号等) フィデリティ証券株式会社
金融商品取引業者 関東財務局長(金商) 第152号
(加入協会) 日本証券業協会

