

簡単に理解できる

Keeper Securityの特別版

適切なパスワード管理とは

for
dummies[®]
A Wiley Brand



サイバー犯罪者から
身を守る

パスワード管理のベスト
プラクティスを学ぶ

オンラインアカウント
や資産を保護する



KEEPER[®]
Cybersecurity Starts Here[®]

提供

ブライアン・アンダーダル

Keeper Securityについて

Keeper Security は、世界中の人々や組織のサイバーセキュリティを変革しています。Keeper の手頃な価格で使いやすいソリューションは、ゼロトラスト、ゼロ知識セキュリティの基礎の上に構築されており、すべてのデバイスにおけるすべてのユーザーを保護します。



パスワード管理

Keeper Security特別版

ブライアン・アンダーल著

for
dummies[®]
A Wiley Brand

目次

導入	1
本書について.....	1
本書で使用されているアイコン.....	1
本書の方向性	2
第1章: サイバー犯罪とハッキングの紹介.....	3
リスクを理解する.....	3
自社の脆弱性を理解する.....	4
マルウェア.....	4
アカウント盗難	5
安全でない接続	6
第2章: パスワードの現状を理解する	7
パスワードがサイバー犯罪の第一の要因である ことを考える	7
パスワードの問題点を考える.....	8
推測やクラックが容易	9
複雑でユニークであれば覚えにくい.....	9
使いにくい	10
第3章: パスワード管理について考える	11
一般的なパスワードの管理方法について.....	11
書き留める	11
Excelスプレッドシートやデータファイル.....	12
Webブラウザに保存する	12
パスワードマネージャー	13
パスワードマネージャーについて理解する	13
第4章: 正しいパスワード管理 ソリューションを見つける	15
個人ユーザーのためのパスワード管理を考える	15
ビジネス向けのパスワード管理を見つける	17
第5章: パスワード管理について覚えておく べき10の事項.....	19

導入

盗難やデータ侵害などのサイバー犯罪は、個人と企業の両方をさらに危険にさらしています。残念なことに、アカウントを保護するために最もよく使用される方法であるパスワードは、サイバー犯罪の最大の原因となっています。なぜなら、高強度のパスワードを使用することは、難しすぎてストレスが溜まり、間違いが発生しやすいからです。このため、個人や企業は、正しい対応を施さずパスワードの問題に対処することがよくあります。たとえば、推測しやすいシンプルなパスワードを設定したり、すべてのオンラインアカウントに同じパスワードを使用したり、モニターの側面に貼った付箋にパスワードを書いたりします。このような方法は、一見問題のない簡単な管理方法に思えますが、実際は、サイバー犯罪者からの被害を受けやすくなってしまいます。人々が自分のアカウントやその他のオンライン資産を保護するために、はるかに安全で便利な方法を必要としているのは明らかです。

本書について

適切なパスワード管理とは、Keeper Securityの特別版では、オンラインセキュリティを大幅に向上させることができるパスワード管理システムについて、知っておく必要があることを学ぶことができます。本書では、適切なシステムを使用することで、余分な労力を必要とせず、オンラインライフを複雑にすることなく、自分自身と自分の資産を守るために非常に強力なパスワードを簡単に使用できる方法を紹介します。

本書で使用されているアイコン



本書では、特に役立つと思われる情報に注意を促すために、以下のアイコンを使用しています。

このアイコンで示された情報は重要であるため、強調するために繰り返されます。こうすることで、後で本を参照するときに、注目すべき情報を簡単に見つけることができます。



このアイコンは、さらに役立つ情報を示しています。



このアイコンは、専門用語など技術的なことが議論される場所を示しています。



警告アイコンが付いている段落は、読者が遭遇する可能性のある一般的な落とし穴に注意を促しています。

本書の方向性

本書はモジュール化されています。本書に書かれていることはどれも重要で興味深いものばかりですが、今すぐすべてを読む時間がない場合でも、特定の章にジャンプして有用な情報を素早く得られるように構成されています。とはいえ、重要な情報を見逃さないように、読み飛ばした章は後で読み返したくなることでしょう。

この本の限られたスペースに、必要な情報をすべて詰め込むことは不可能でした。最新のニュースや情報については、https://www.keepersecurity.com/ja_JPを参照してください。

- » リスクを理解する
- » 自社の脆弱性を把握する

第一章

サイバー犯罪と ハッキングの紹介

サイバー犯罪は、オンラインの世界を危険な場所へと変貌させています。この章では、私たちが直面するリスクについて見ていき、私たちが攻撃される可能性のある方法をいくつか考えていきます。これらの問題を理解することで、個人と企業を守ることがいかに重要であるかを理解することができます。

リスクを理解する

データ漏洩などのサイバー犯罪の件数、規模、コストは急速に増加し、個人や企業にかかわらず、サイバー犯罪者は日々チャンスを狙っています。コンピュータセキュリティの専門家でない限り、どのようなリスクにさらされているのが見えないかもしれません。では、次のことを考えてみてください：

- » **法的責任：** ビジネスを運営している場合、個人情報、クレジットカード、購入した製品などの機密情報を含む顧客データを保護する責任があります。ほとんどの司法管轄区では、データ侵害の結果生じる費用は、顧客ではなく事業者が負担します。

- » **ビジネスの損失：**データ漏洩を経験した企業は、顧客の維持に苦勞することが多くあります。自分のデータを守ってくれる企業だと信頼できないと感じれば、顧客は他へ取引を移すでしょう。
- » **安全でないデバイス：**あなたの情報にアクセスできるすべてのデバイスは、不正アクセスの可能性を秘めています。家で不在の際に、玄関のドアを大きく開けっ放しにしないのに、安全でないスマートフォンやノートパソコンのようなデバイスを使って銀行口座にアクセスするのは危険です。
- » **個人情報の盗難：**IDを盗む犯罪者は、あなたの人生を地獄に変えることだって可能です。もちろん、不正に利用された口座は解約できますが、支払督促に直面し、請求書を出したのが自分ではないことを証明するのに何百時間も費やすことになります。
- » **知的財産：**ビジネスには、特許、商標、企業秘密など、第三者の手に渡っては困る知的財産があるでしょう。そのような資産が、適切に保護されていることを確実にする必要があります。資産を保護するために対策を講じたとしても、攻撃を受けた場合の後始末に比べれば、問題を未然に防ぐ方がはるかに容易です。データ漏洩やサイバー攻撃から回復することは、問題を未然に防ぐことよりも非常に難しく、費用もかかります。



自社の資産を守るためにいくら努力しても、被害にあった場合の後始末に比べれば、問題を未然に防ぐ方がはるかに簡単であることには変わりはありません。データ漏洩やサイバー窃盗から回復することは、そのような問題を未然に防ぐことよりも常に難しく、費用もかかります。

自社の脆弱性を把握する

リスクを軽減するためには、どこがどのように脆弱なのかを理解する必要があります。残念ながら、今日のインターネット社会では、多彩な方法で攻撃を受ける可能性があります。この章では、その攻撃のいくつかを見ていきます。

マルウェア

マルウェアとは、悪意を持って設計されたソフトウェアのことを指します。コンピュータウイルス、トロイの木馬、ランサムウェアは、マルウェアの一般的な例です。

マルウェアはさまざまなソースからやってきます：

- » 不正にインストールされたソフトウェア
- » 感染したウェブサイト
- » 無料の便利なものを装ったアプリケーション



どこかに転がっているUSBキーを挿入してはいけません。マルウェアの作者は、人々がUSBキーに何が入っているかを確認するためにUSBキーを挿入することを知っており、キーが挿入されるとすぐに自動的にインストールされるマルウェアを作成するのは簡単です。

口座盗難

口座盗難は、誰かがあなたの機密情報にアクセスしたり、多額の買い物をしたり、銀行口座を完全に流出させたりする可能性があります。多くの場合、問題に気づく前に大きな被害が発生してしまいます。ほんの数分しかかからないのです。



ほとんどのオンラインアカウントは、ユーザー名とパスワードを要求することでアクセスを管理しています。その多くは、メールアドレスがユーザー名を兼ねています。しかし、ユーザー名を別に持っている場合でも、ユーザー名は公開されていることが多くあります。事実、ユーザーは推測しやすいユーザー名でログインし、アカウントを保護するためにかなり弱いパスワードに頼るのが一般的です。長くて複雑なパスワードの方が、単純で短いパスワードよりもはるかに安全です。



しかし、強力なパスワードであっても、二段階認証を使うシステムよりは安全性が低いです。基本的に、二段階認証は、テキストメッセージで送られたコードを入力するなどの確認ステップを追加するか、あなたが本当に本人であることを証明する別の手段を追加します。アカウント窃盗によく使われるマルウェアの一種に、キーロガー（ユーザーのキー入力を記録するソフトウェアの一種）があります。キーロガーの中には、ログイン画面を監視してユーザーの入力を記録し、その情報をリモートサーバーに送信するものもあります。

安全でない接続

インターネット上では、情報がプレーンテキストで送信されることが多くあります。インターネットのトラフィックを盗み見る者は、その情報をいとも簡単に読み取ることができます。ユーザー名、パスワード、アカウント番号、その他の機密情報がこのような安全でない接続で送信された場合、その情報を盗むことは簡単なことです。



機密情報を入力する前に、ブラウザのアドレスボックスでURLの先頭にhttpsがあるかどうかを常に確認してください。httpsは、httpで始まるアドレスのようにプレーンテキストではなく、接続が暗号化されていることを示しています。また、ほとんどのブラウザでは、暗号化された安全な接続にはロックアイコンが表示されます。



利用可能なソフトウェアのパッチやアップグレードを無視することも、自分自身を危険にさらすことになります。ソフトウェア会社は、発見された脆弱性の修正パッチを発行することがよくありますが、ユーザーがそのパッチを適用しない場合、ソフトウェアを実行しているデバイスが攻撃の標的になる可能性があります。

- » パスワードがサイバー犯罪の第一の原因であることを考える
- » パスワードの課題を考える

第2章

パスワードの現状を理解する

オンラインアカウントやデジタル資産を保護することは、現代社会では絶対に欠かせません。世の中には、盗めるものは何でも盗もうと平気でする者が大勢いますので、無防備になるリスクを負う余裕など誰にもありません。多くの場合、オンライン資産はユーザ名とパスワードで保護されています。この章では、パスワード保護の現状に目を向け、一般的なパスワードの使い方がいかにあなたを危険にさらしているかをご紹介します。

パスワードがサイバー犯罪の第一の原因であることを考える

コンピュータの黎明期には、パスワードはあまり重要ではありませんでした。コンピュータは巨大で集中管理されたデバイスであり、ほとんどの人が目にすることはありませんでした。初期のコンピュータに近づくには、厳重に警備された鍵のかかった部屋に物理的にアクセスする必要がありましたし、いったん中に入ると、何かをするには難解なプログラミング言語を知っている必要がありました。このような困難なアクセスに加え、初期のコンピュータのほとんどは完全にスタンドアロンで、外部との接続がありませんでした。インターネットもオンラインアクセスも存在しませんでした。

今日ではもちろん、事実上すべてのコンピュータデバイスがインターネットに接続されています。PC、ノートパソコン、タブレット、スマートフォン、そして一部の家電製品もインターネットを介して通信するようになっています。この接続性は、デジタルリソースへのアクセスを完全に管理することが絶対不可欠になったことを意味します。

アクセス制御がこれほど重要になると、ユーザー名とパスワードさえあれば、問題がないように思われます。それでは、ユーザー名と正しいパスワードの組み合わせというのは、推測が困難でなければならないのではないのでしょうか？

しかし、実際の数値を見てみると、必ずしもそれが守られていないことを示しています。中小企業を対象とした最近の調査によると、半数以上の企業が過去1年間にサイバー攻撃の標的になったことがあるといいます。このようなサイバー攻撃は、ユーザー名やパスワードといった現在の保護手段が脆弱であればあるほど成功率が上がります。



ユーザー名とパスワードの正しい組み合わせを思い出すのは難しいと思うかもしれませんが、その組み合わせの半分であるユーザー名は、メールアドレスやパブリックフォーラムにおけるユーザーのオンラインIDなど、公開情報であることが多いことを覚えておきましょう。さらに、多くの異なるアカウントで全く同じユーザー名を使用することは極めて一般的です。その結果、ハッカーはユーザーのパスワードをあらゆる方法で推測するだけで、フルアクセスできるようになってしまいます。

パスワードの課題を考える

オンライン資産を保護することは、当然ながら非常に重要です。ショッピングモールに買い物に行くとき、駐車場に鍵のかかっていない車のエンジンをかけたままにしようとは思わないでしょう。同様に、今日の危険なインターネットの世界では、アカウントやその他のオンライン資産を保護する対策を講じる必要があります。残念ながら、オンライン資産を保護するためにパスワードを使い管理を怠ると、多くの大きな問題が発生します。

パスワードの課題を考える

”パスワード”や”12345”というような単純な単語をパスワードとして使ったことがありますか？簡単なパスワードを使っていないなら、自分を褒めてあげましょう。なぜなら、これらは人々がよく使うパスワードの一部だからです。実は、人々が最もよく使うパスワードのリストがオンラインで公開されているのです。よって、パスワードを推測しようとする人は、ほとんどの場合、かなり簡単に推測できてしまうのです。

なぜ人々は推測されやすい単純なパスワードを使うのでしょうか？実に簡単です。サイバーセキュリティをあまり真剣に考えていない人にとって、パスワード管理というのは厄介なものなのです。結局のところ、誰が自分の情報を盗みたいと思うのかと勝手に思い込み、必要以上の努力をしたくはないのです。しかし、パスワード管理は厄介でも我慢して正しい対策や管理をしなければならないのです。



また、いくつもの異なるアカウントでパスワードを再利用することは、サイバー犯罪者にとって誰かのパスワードを推測することを非常に簡単にしてしまいます。実際、サイバー犯罪者はあるアカウントで使えるパスワードを見つげると、すぐに同じパスワードを試して、他のアカウントにアクセスできるかどうかを確認します。もちろん、複数のアカウントで同じパスワードと同じユーザー名を使用している場合、1つのラッキーな推測が成功したことで、サイバー犯罪者はそれらのアカウントすべてにアクセスできてしまいます。



パスワードポリシーが厳格に実施されていないことが多く、このような見落としが、ユーザーが脆弱で推測しやすいパスワードを設定することを可能にしているのです。ビジネスを経営していたり、パスワードを管理する立場であれば、パスワードポリシーが強制可能で、強力なパスワードを要求するものであることを確認する必要があります。パスワードポリシーに強制力を持たせ、強力なパスワードを要求しましょう。最低限、パスワードの長さや複雑さに関するルールを設定できるシステムを利用しましょう。

複雑でユニークであれば覚えにくい

多くの専門家は、大文字、小文字、数字、特殊文字を組み合わせた、長くて複雑なパスワードを使うことを勧めています。特に、パスワードに普通の単語が含まれていない場合、パスワードに余分な文字があればあるほど、そのパスワードを推測するのが難しくなります。例えばjoH8243_sMitH\$mEのようなパスワードは、おそらく誰かがハックすることは事実上不可能でしょう（しかし、ここでこれを使ってしまったので、おそらくハッカーの持つパスワードリストに追加されるでしょう。）



残念ながら、joH8243_sMitH\$mEのようなパスワードは覚えるのも非常に難しく、モニターの横に貼った付箋紙（またはパスワード用のお気に入りの場所）に書き留めなくなるかもしれません。あるいは、パスワード付箋のお気に入りの場所である、机の引き出しの一つにメモしたくなるかもしれません。もちろん、付箋でパスワードを記録することは誰でもやりがちなことなので、パスワードを管理する方法としてはあまり安全とは言えません。すべてのデータを暗号化する優れたパスワードマネージャー・システムを使えば、複雑で解読が難しいパスワードをずっと簡単に使えるようになります。パスワードマネージャーはパスワードを保存するだけでなく、見せないように非公開にすることもできます。高性能のパスワードマネージャーには、安全なパスワードの自動生成や、様々なサイトやアカウントへのログイン情報の自動入力などの機能も含まれていることが多々あります。

使いにくい

最後に、強力なパスワードは覚えにくだけでなく、正しく入力するのも難しいため、使いにくい場合があります。文字が組み合わせさった長くて複雑なパスワードを使うと、パスワードの入力を簡単に間違えてしまいます。



ほとんどのサイトでは、パスワード入力欄の内容が隠されているため、間違ったパスワードを入力したことを知らされても、どのような間違いなのかわからないことがあります。また、正しいパスワードを入力するための試行回数が限られているサイトでは、本当に複雑なパスワードを使用するとイライラすることがあります。パスワードを自動入力してくれる優れたパスワードマネージャーを使うことは、このようなイライラを避ける効果的な方法の一つです。



同じ複雑なパスワードを何度も再利用できると思ってはいけません。先に述べたように、誰かがあなたのパスワードを発見した場合、彼らはあなたがアカウントを持っている他のサイトで同じパスワードを試す可能性が高いので、注意しないといけません。

- » 一般的なパスワード管理方法
- » パスワードマネージャーを理解する

第3章

パスワード管理を考える

人口の80%以上がインターネットを利用する現代社会では、何十、何百ものユーザー名とパスワードを個人で所有しています。それらをすべて覚えようとする、不可能ともいえる作業になります。この章では、パスワードを管理するために一般的に使われている方法をいくつか紹介します。なぜ安全なパスワード管理ソリューションに切り替えた方がいいのかを考えましょう。

一般的なパスワード管理方法

人々は様々な方法でパスワードを管理しています。多くの場合、以下のような方法でパスワード管理を行い、中にはまったく安全ではなく、盗難や悪用を招きかねない方法もあります。

書き留める

パスワードを記録するために人々が使う最も一般的な方法は、おそらく紙に書き留めることでしょう。その紙は、コンピュータのモニターの横に貼った付箋だったり、机の一番上の引き出しに貼ったメモだったりします。いずれにせよ、たまたま通りかかった人が「偶然」目を通してパスワードを読んでしまう可能性があります。



あるITマネジャーは、パスワードを書いたメモをデスクに置いておくユーザーを思いとどらせる方法を考えつきました。彼はオフィス内を歩き回ってこれらのメモを探し、見つけたらそのアカウントにログインしてパスワードを変更し、アカウントからロックアウトしました。そして、ヘルプデスクへの電話をきっかけに、パスワードのセキュリティについて講義したのです。

Excelスプレッドシートまたはデータファイル

パスワードを管理するもう一つの一般的な方法は、様々なアカウントのユーザー名とパスワードをExcelのスプレッドシートやデータファイルに記載することです。この方法は、書いたメモを使用するよりも若干良いように思えるかもしれませんが、これらのファイルは平文として保存され、多くの場合、"passwords"のような明白なファイル名を使用します。



Excelのスプレッドシートやデータファイルは通常暗号化されていないため、ファイルにアクセスできる人なら誰でも、すべてのユーザー名とパスワードに完全にアクセスできてしまいます。また、ファイルのコピーを入手するためにあなたのノートパソコンを盗む必要はありません。特に、あなたのネットワーク上でファイルを見つけたり、コーヒーを飲みに行くときにデバイスのロックを解除したままにしておいたりする場合はなおさらです。

ウェブブラウザに保存

最近のウェブブラウザの多くは、アクセスしたサイトのユーザー名やパスワードを記憶してくれる便利な機能を備えています。この機能は便利のように思えますが、あなたのコンピューターにアクセスした人は、あなたのオンラインアカウントにもアクセスできてしまうため、この機能を使うことは大きなリスクを負うことになります。また、この機能は、情報が作成されたデバイスにのみ保存されたり、読みやすい平文として保存される場合もあるため、複数のデバイスを使用している場合には不便です。



ウェブブラウザにアカウントログインを記憶させる場合は、コンピューターにログインする際にパスワードまたは生体認証スキャンが必要になるように、システムを設定することが重要です。さらに、たとえ数分間であっても、外出するときは必ずログアウトするか、少なくともコンピューターをロックしてください。

パスワードマネージャー

正しい方法で仕事をしたいのであれば、その作業のために特別に設計されたツールを使った方がはるかに良い結果が得られるでしょう。パスワードを安全に管理することに関しては、実際のパスワードマネージャーに勝るものはありません。パスワードマネージャーについて詳しくご紹介します。

パスワードマネージャーを理解する

オンライン上で自分自身や自分の資産を真剣に守ろうと思ったら、専用のパスワードマネージャーを検討する必要があります。中途半端な対策ではなく、安全性とセキュリティを確保するために必要な機能をすべて盛り込んだものが真のパスワード管理です。

パスワードマネージャーは、ユーザー名とパスワードを安全に暗号化して保存します。個人、家族、そしてあらゆる規模の企業のニーズを満たすために、様々なニーズに合わせて利用可能です。包括的なパスワードマネージャーは、ユーザー名とパスワードを保存するだけでなく、各アカウントごとに非常に強力なパスワードを自動生成することも可能です。しかし、優れたパスワードマネージャーは、サイトを自動的に認識し、ユーザー名とパスワードを安全に入力し、強力なパスワードを生成するだけではありません。

優れたパスワードマネージャーは、強力なパスワードを簡単に生成し、容易に使えるような機能が備えられています。個人がパスワードを覚えておく必要もなく、アカウントにログインするために複雑なパスワードを入力しようと苦勞する必要もありません。



幅広いプラットフォーム、オペレーティングシステム、ストレージ機能に対応しているパスワードマネージャーを探しましょう。Android、iPhone、BlackBerry、Windows Phone、iPad、Microsoft Surface、Amazon Kindle、Mac、Linux、Windows PCをサポートしているものが良いでしょう。



ほとんどのパスワードマネージャーは暗号化されており、パスワードにアクセスするためにはアプリケーションにログインする必要があります。パスワードマネージャーは、暗号化されたデジタル保管庫に情報を保存します。本当に安全なソリューションを選ぶことが重要です。セキュリティにおける重要な要素は、ゼロ知識として知られているものです。これは、データの暗号化と復号化を完全にコントロールできるのはユーザーだけであることを意味します。データを復号化するために必要な暗号化キーは、常にユーザーの手元に残ります。これにより、パスワードマネージャーの提供元やクラウドストレージプロバイダーを含む他の誰であっても、ユーザーのデータを復号化することができません。

ゼロ知識アプローチが重要なのは、オンラインに保存されたデータがハッキングされたとしても、ハッカーはそれを解読できないからです。さらに、このアプローチでは、データが転送中も暗号化されたままであることが保証されるため、誰かがインターネットを横断するデータストリームを盗聴することに成功しても、データを復号化することはできません。

多くの組織では、データを安全に保存する必要性はパスワードだけに留まりません。これには、Secure Shell (SSH) キー、デジタル証明書、さまざまな機密ビジネス文書、ファイル、ビデオ、写真などが含まれます。したがって、パスワード管理ソリューションの推奨機能は、これらの追加タイプの情報を安全に保存できることです。



また、より優れたソリューションの中には、単純なユーザー名とパスワードよりもはるかに優れたセキュリティを提供する二要素認証を採用しているものもあります。二要素認証は、次のようなセキュリティのレイヤーを追加します。生体認証スキャン、テキストメッセージとして送信されるコードの入力、またはGoogle Authenticatorのような物理的または仮想的なワンタイムパスコードジェネレーターからのコードの提供をユーザーに要求します。

- » 個人ユーザーのためのパスワード管理を考える
- » ビジネス向けのパスワード管理を見つける

第4章

正しいパスワード管理 ソリューションを見つける

適切なパスワード管理ソリューションを見つけることは重要です。慎重に選び、自分を守り、ニーズに合い、使いやすく、予算に合ったソリューションを選ぶようにしましょう。この章では、個人ユーザーと企業がパスワード管理に何を求めるべきかについて説明します。

個人ユーザーのための パスワード管理を考える

優れたパスワード管理ソリューションが必要なのは、企業だけではありません。個人情報盗難のようなサイバー犯罪からの保護も個人ユーザーには必要です。個人や家庭には、オンラインセキュリティのニーズに対応するITスタッフがいないことを考えれば、個人ユーザーがあらゆる支援を必要としていることは明らかです。

個人ユーザーとしては、特許、商標、独自の企業秘密などの知的財産を守る必要はないかもしれませんが、銀行口座、医療記録、オンラインアカウント、貴重な家族の写真など、安全に保ちたい資産はたくさんあります。例えば、個人情報を盗まれた場合、その修正に数千ドルと数え切れないほどの時間を費やすことになります。パスワードマネージャーを使うことで、そのような事態を一つでも防ぐことができるのであれば、その価値はあるのではないのでしょうか。

適切なパスワードマネージャーを見つけるのはそれほど難しいことではありませんが、以下のような機能を探してみてください：

- » **パスワードの保存：**パスワードマネージャーを使う一番の理由は、二度とパスワードを覚えなくてすむことです。また、パスワードを覚える必要がなければ、より簡単に複雑で強力なパスワードを使うことに障害はなく、アカウントの安全性を高めることができます。
- » **生体認証を活用する：**お使いのデバイスに指紋認証が搭載されている場合、パスワードマネージャーを利用して生体認証機能を活用することをお勧めします。全てのパスワードマネージャーがこれらの機能を利用できるわけではありません。
- » **パスワードの生成：**正直なところ、人々はランダムな文字で構成された強力なパスワードを考え出すのが苦手です。推測が事実上不可能な、強度の高いランダムなパスワードを作成できるパスワードマネージャーが必要です。
- » **簡単なログイン：**優れたパスワードマネージャーは、ログイン認証情報の自動入力が可能です。この機能により、入力を間違えて何が間違っているのかを見つけたり、アカウントからロックアウトされたりすることがなくなるため、強力なパスワードの扱いがはるかに簡単になります。
- » **デジタル保管庫：**保護する必要があるのはパスワードだけではないため、プライベートファイル、写真、ビデオを安全なデジタル保管庫に保存できるパスワードマネージャーを検討することをお勧めします。
- » **複数のデバイスのサポート：**現在所有しているすべての種類のデバイスで動作し、1つのプラットフォームに固執しない柔軟性を備えたパスワードマネージャーが必要です。複数デバイスのサポートの重要な部分は、それらのデバイス間の自動同期です。デスクトップPCに新しいアカウントとパスワードを追加した場合、スマートフォンやタブレットでも、きっとその情報にアクセスできるようにしたいと思うでしょう。

- » **二段階認証**：ユーザー名とパスワード以上の認証情報を必要とする場合、誰かがあなたのアカウントに侵入することははるかに困難となるため、二段階認証を使用するパスワードマネージャーを検討することをお勧めします。
- » **簡単な共有**：もう1つの優れた機能は、友人や家族とファイルを安全に共有できることです。一部のパスワードマネージャーでは、このオプションが提供されています。



家族全員を保護するには、ファミリー プランを提供するパスワードマネージャーを探すことを検討してください。デジタルセキュリティをあまり真剣に考えていない家族に気を配るだけでなく、ファミリー プランを利用すると費用も節約できる可能性があります。さらに、家族全員を参加させることで、自分の資産を保護することの重要性について貴重な教訓を与えることができます。

ビジネス向けのパスワード管理を見つける

ビジネスを経営している方は、従業員、顧客、ビジネス資産が直面する多くのリスクをすでに認識しています。また、サイバー犯罪があらゆる規模のビジネスに影響を与えることもご存じでしょう。ビジネスに影響を与えるデータ侵害の74%以上は、脆弱なパスワードとポリシーが原因であると推定されています。適切なパスワード管理ソリューションは、これらの問題を最小限に抑えるように回避するのに役立ちます。

前述した 個人ユーザー向けパスワードマネージャーに必要な機能のほとんどは、企業向けソリューションでも非常に望ましいものです。明らかに高強度のパスワード、使いやすさ、安全な認証などが、ビジネスのパスワード管理ソリューションに求められる機能です。ただし、これらに加えて、次のような機能も探してください。

- » **管理者用ダッシュボード**：強力なパスワード ポリシーを適用し、従業員のポリシー遵守を監視できるソリューションが必要です。また、堅牢なレポート機能と監査機能、また潜在的な問題を警告する通知も必要です。

- » **特権アカウント管理：**給与記録やその他の機密情報などの特定のデータには、アクセスを制限する必要があります。パスワードマネージャーで特権アカウントの認証情報のライフサイクルを安全に管理し、役割ごとのアクセス許可を設定し、認証情報の共有を制御し、スケジュールされたパスワード変更を強制できることが重要です。
- » **ヘルプデスクのコストの削減：**パスワードを紛失したユーザーを支援する必要性を減らすシステムが必要になります。
- » **簡単な拡張性：**ビジネスの成長に合わせて成長できないシステムにとらわれたくありません。現在や今後のビジネスニーズに簡単に対応できるシステムが必要です。
- » **迅速な導入：**ビジネスを運営しなければならず、設計が不十分で複雑なシステムの実装に時間を無駄にするわけにはいきません。現在や将来のビジネスの規模に関係なく、直感的で導入が簡単なシステムを探してください。
- » **安全な共有：**管理者が会社のポリシーと内部統制へのコンプライアンスを維持できるように、構成可能な権限とポリシーを使用して、チーム全体で個々の記録と暗号化されたフォルダーの両方を安全に作成、共有、管理する必要があります。
- » **企業の構造およびポリシーとの整合性：**セキュリティソリューションは、企業の構造やポリシーに適応できるかどうかによって決まります。独自の環境に完全に適合させるためには、構成可能な役割、その役割ごとの権限や管理者特権が必要です。これらはすべて、特定の組織階層によって自在に割り当てが可能です。
- » **パスワードの衛生管理とパスワード使用状況レポートの可視性：**ほとんどの企業では、従業員のパスワードの使用状況の可視性が限られており、サイバーリスクが大幅に増加しています。パスワードの使用とコンプライアンスに関する重要な情報がなければ、パスワードの衛生状態を改善することはできません。

第5章

パスワード管理について 覚えておくべき10の事項

この章では、パスワード管理について覚えておきたい10の簡単な事実をまとめます。

- » 個人情報 (PII) と財務情報は、最も貴重な資産の1つです。金融口座、機密文書、パスワード、および ID はオンラインに保存されているため、ハッキングされる危険性があります。ハッカーはサイバー攻撃を行う際に個人情報を標的にしており、この情報から年間数千億円を稼いでいます。
- » 企業や個人に対するサイバー攻撃が増加しています。自分が標的になるかもしれない危険性がいつもつきまとっています。
- » パスワードの粗悪な管理はサイバー攻撃の最大の原因です。簡単に推測できない強力なパスワードを使用する必要があります。

- » 強度の高いパスワードを手動で生成、保存、管理することは難しく、時間がかかり、エラーが発生しやすいため、多くの場合、ストレスや生産性の欠如につながります。
- » より優れたセキュリティが必要です。暗記、付箋による保管、スプレッドシートへの保存などの一般的なパスワード管理ソリューションは、安全ではなく非効率的です。
- » アカウントとデバイスの数が増加することで、パスワードに対するセキュリティが複雑になります。複数のデバイスで多数のオンラインアカウントのパスワードやその他の個人情報を管理することが、ますます困難になってきています。
- » Keeperのパスワードマネージャーは、パスワード管理の課題を解決し、オンラインの生産性を向上させながら、サイバー攻撃のリスクを軽減します。
- » 個人にもパスワード管理が必要です。個人や家族は、デジタルライフを簡素化して保護し、パスワードやその他のデジタル資産を友人や家族と共有する、簡単な方法を提供するパスワードマネージャーを必要としています。
- » ビジネスには情報の保護が必須です。企業は、データ侵害のリスクを大幅に軽減し、安全なパスワード管理を簡素化し、ますます個人所有デバイスの持ち込み (BYOD) が進む職場環境で生産性を向上させ、パスワードポリシーの適用とパスワード管理を可能にするパスワードマネージャーを必要としています。パスワードマネージャーは、パスワードの衛生状態と職場内での慣行を監視します。
- » すべてのパスワードマネージャーが同じように作られているわけではありません。強力なパスワードを簡単に使用でき、生体認証を使用でき、自動アカウントログインが可能で、幅広いデバイスをサポートするパスワードマネージャーを探してください。



Keeperのパスワード管理ソリューションの無料トライアルは、<https://keepersecurity.jp> から開始できます。

Password Management For Dummies[®], Keeper Security Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2017 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Trademarks: Wiley, For Dummies, the Dummies Man logo, Dummies.com, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Keeper and the @Keeper logo are registered trademarks of Keeper Security, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom For Dummies book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the For Dummies brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-38973-6 (pbk); ISBN 978-1-119-38974-3 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Senior Acquisitions Editor:

Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative:

Katie Helm

Production Editor: Magesh Elangovan



パスワードに関連するデータ漏洩や
サイバー脅威を防止する、サイバーセキュリティ・
プラットフォームのリーディングカンパニー

keepersecurity.com

サイバー犯罪から身を守る

サイバー犯罪は、個人のみならずビジネスまでも、ますます危険にさらしています。残念なことに、アカウントを守るための方法であるパスワードが、情報漏洩などのサイバー犯罪の主な要因となっています。ここではオンライン上のセキュリティと生産性を大幅に改善することのできるパスワード管理方法について知っておくべきことを解説しています。強力なパスワードの正しい管理方法を知ること、安心して効果的にオンライン活動を行うことにつながります。

内容

オンライン上に潜む脅威を理解する
パスワード管理について学ぶ
ビジネスまたは個人での解決策を見つける
複雑で強力なパスワードを作成する
個人情報盗難から自身を守る
従業員と顧客を守る
パスワードを覚えるという作業を失くす！



ブライアン・アンダーダル is a well-known author and technologist who enjoys making complicated topics easy for ordinary people to understand.

Go to [Dummies.com](https://dummies.com)[®]
for videos, step-by-step photos,
how-to articles, or to shop!

for
dummies[®]
A Wiley Brand

ISBN: 978-1-119-38973-6
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.