特集

不正アクセス被害急増中！
ーあなたの対策、アップデートできていますか？

特集1

不正ログインの脅威と対策
ー巧妙化するフィッシングに対応する方法とは？

神谷 健司 Kamiya Kenshi
独立行政法人情報処理推進機構（IPA）
セキュリティセンター普及啓発・振興部　相談・支援グループ エキスパート

不正ログインとは、第三者が不正に入手したIDおよびパスワードを使用し、正規の利用者になりすましてインターネットサービス等に不正にログインする行為を指します。不正アクセスと呼ばれることもありますが、本稿では「不正ログイン」という用語を使い、その手口と対策について解説します。

不正ログイン被害の現状

独立行政法人情報処理推進機構（以下、IPA）の「情報セキュリティ安心相談窓口」（以下、安心相談窓口）[*1]には、不正ログインによるSNSアカウントの乗っ取り被害の相談が数多く寄せられています。SNSアカウントの乗っ取りとは、Instagram等のアカウントに不正ログインされ、不正ログインした相手にパスワードを変えられて、アカウントの所有者がログインできなくなることです。乗っ取られたアカウントから、不審な商品やサービスを宣伝する投稿をされてしまうことがあります。この場合、自分のアカウントが不審な投稿のために悪用されていることを目の当たりにしながら、それを止めることができません。そのため、被害者にとって精神的な苦痛（被害）になります。こうした中、IPAでは「安心相談窓口だより」にて不正ログインの注意喚起を行いました[*2]。

また、証券口座に不正ログインされ、不正な株の取引をされるという被害が大きな問題になっています。この手口では、「アカウントの悪用」による金銭的被害が発生していると言えます。このように、不正ログインによるアカウントの悪用は、さまざまな被害をもたらします。

不正ログインの手口

ID・パスワード認証への攻撃

SNS等の会員制のインターネットサービスを利用するためにログインする際には、まず利用したいサービスに利用者本人であることを証明する手続きが必要です。この手続きを「認証」と呼びます。従来の認証では、ログインしたいサービスに、IDとパスワードを入力します。パスワードは、本人しか知らない秘密の合い言葉のようなものです。パスワードを使ってサービスに対して利用者本人であることを証明します。

IDは、サービスが利用者を識別するための会員番号のようなものです。会員番号の代わりにメールアドレスや携帯電話番号が使われることが多く、これは本人しか知らない秘密の情報ではありません。そのため、ID・パスワードを使用した認証方式では、パスワードが利用者本人であることを証明する唯一の秘密の情報です。

また、パスワードは部屋の鍵のようなものとも言えます。鍵が１つしかない場合、それを盗まれると不正ログインを許してしまうことになります。ID・パスワード認証では、この「鍵が１つしかない」という点が弱点です。不正ログインを行

*1　IPA「情報セキュリティ安心相談窓口」https://www.ipa.go.jp/security/anshin/index.html
*2　IPA「安心相談窓口だより：インターネットサービスへの不正ログインによる被害が増加中ーパスキー認証や多要素認証の設定を行いましょうー」https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html

う攻撃者（悪者）は、この弱点を悪用するためにパスワードを盗もうとします。では、どのようにしてパスワードを盗むのでしょうか？代表的な手口として、以下のものがあります（詳細は＊2を参照）。

①パスワードを構成するすべての文字の組み合わせを試す「**総当たり攻撃**」
②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**」。”password123”のような、単純な単語と数字の組み合わせをパスワードに使っていると、この手口の被害に遭う可能性があります
③漏えいしたパスワードのリストを使った「**リスト型攻撃**」。同じパスワードを複数のサービスで使い回していると、この手口の被害に遭う可能性があります
④実在する事業者（銀行、証券会社、ネットショップ等）をかたる、偽のメールやSMS（ショートメッセージ）のURLリンクをクリックさせ、本物そっくりの偽サイトに誘導してパスワードを入力させる「**フィッシング**」（**図表1**）

不正ログインの対策

1. 安全なパスワードの設定

①総当たり攻撃や②辞書攻撃への対策は、パスワードを簡単に探り当てることができないようにすることです。そのためには、パスワードは「できるだけ『長く』、『複雑』にし、複数のサービスで『使い回さない』ようにする」必要があります。これを「安全なパスワード」と呼びます。また、「パスワードを使い回さない」ことによって、③リスト型攻撃の対策にもなります。

2. ID・パスワード認証のリスク

「安全なパスワード」の設定によって、代表的な攻撃手段①②③の対策ができました。しかし、④フィッシングに対しては有効な対策になりません。フィッシングはパスワードそのものを盗む攻撃であるため、どれだけ「長く」、「複雑」なパスワードを設定しても不正ログインを防ぐことができません。フィッシングは、不正ログインにつながる最大の脅威です。

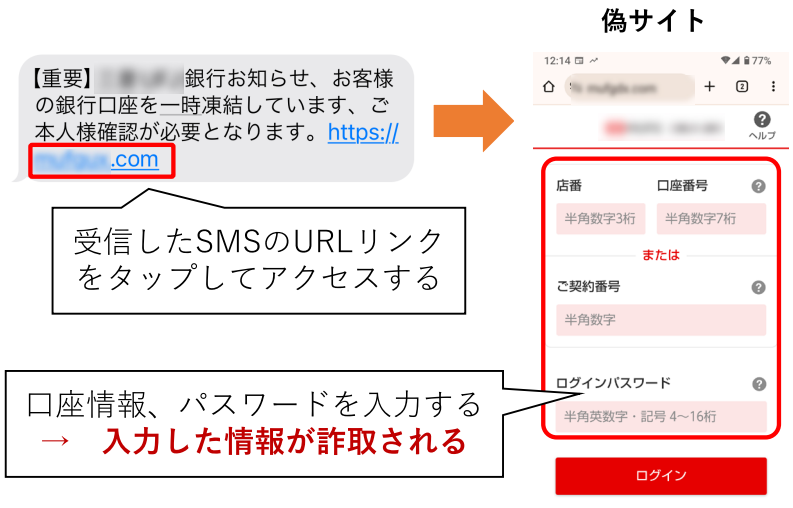
3. ID・パスワードの認証のリスクに対応した「多要素認証」

多要素認証では、利用者本人であることを証明する情報を複数持てるようにしています。部屋の鍵が複数あるようなものです。何者かが、鍵を1つ盗んでも部屋に入ることができないようにすることが、フィッシングの対策になります。

多要素認証の例として、パスワードに加えて、ログインごとに変わるその場限りの「ワンタイムパスワード」を使用する方法があります。ワンタイムパスワードは、SMSを使ってスマートフォンに送信する方法や、スマートフォンの認証アプリを使用して生成する方法があります（**図表2**）。

パスワードは自身が記憶するものですが、ワンタイムパスワードは自身の持ち物であるスマートフォンに表示されます。これは、利用者本人であることを証明するために、「自分だけが知っている記憶を根拠にする」ことに加えて、「自分だけの持ち物を根拠にする」という要素を加えたことを意味します。このように、利用者本人を証明する際の根拠

図表1　フィッシングによるパスワードの詐取



となる認証要素を複数使う方法を「多要素認証」と呼びます。

この方法を使うと、パスワードとスマートフォンの２つが鍵となり、２つを同時に盗まれない限り不正ログインができません。そのため、パスワードを盗むフィッシングの対策になります。

図表２に示したSMSを使用した多要素認証では、「記憶」と「持ち物」という認証要素を使いました。これ以外に、「本人自身を示すもの」である「指紋」や「顔」を認証要素として使用することもあります。

4. 多要素認証を破る「リアルタイムフィッシング」攻撃の出現

リアルタイムフィッシングでは、不正ログインを行う攻撃者が、偽サイトに入力させたID・パスワードをその場で抜き取って正規サイトに入力します。被害者に多要素認証のワンタイムパスワード（**図表３**ではOTPと略）が届くと、それを偽サイトに入力させて、すぐにその抜き取ったワンタイムパスワードを正規サイトに入力します。

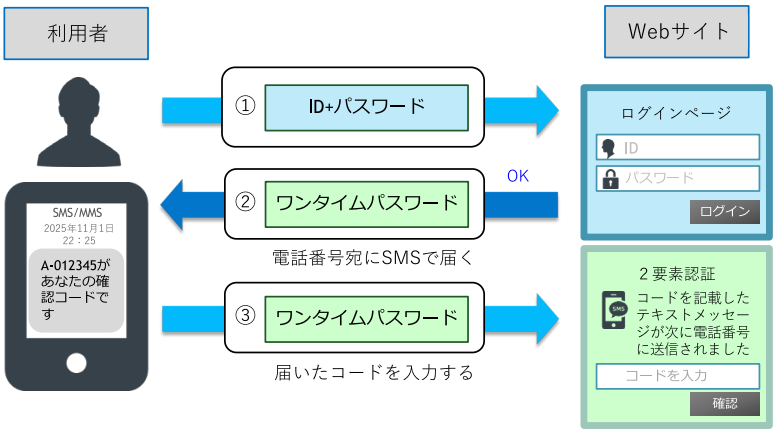
このように、認証情報を盗み、その場で不正ログインに悪用するため、リアルタイムフィッシングと呼ばれています（**図表３**）。リアルタイムフィッシングを使われると、ワンタイムパスワードを使用した多要素認証を破られてしまいます。

5. フィッシングのリスクに対応したパスキー

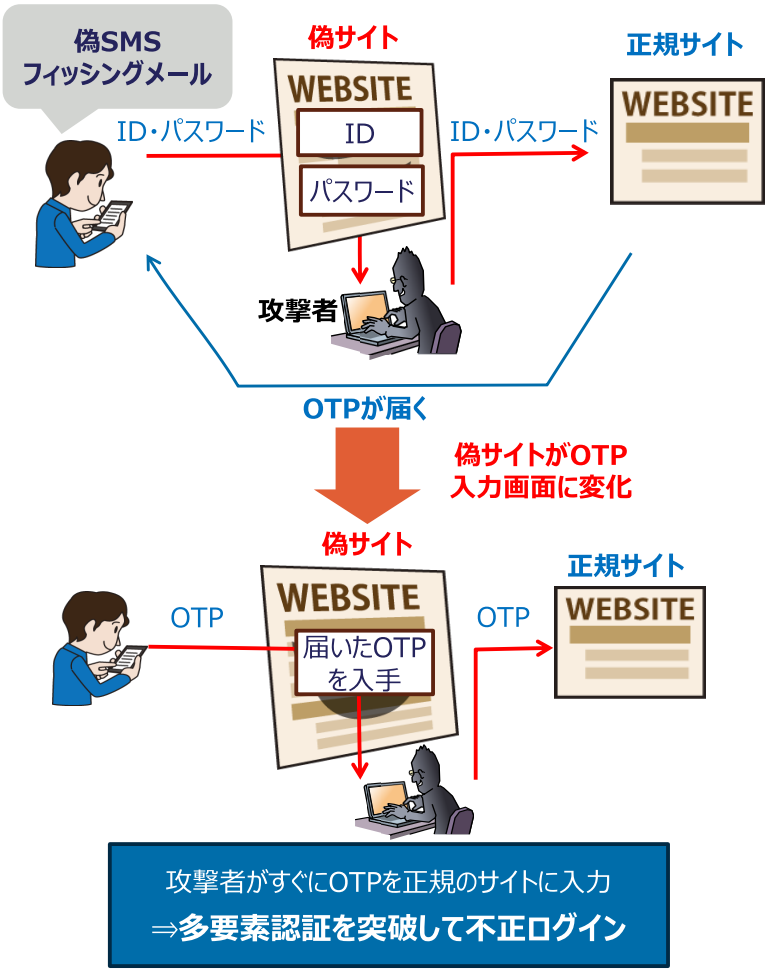
リアルタイムフィッシングは、誘導された偽サイトに、パスワードとワンタイムパスワードの両方を入力させられ、それらを盗まれることで発生します。そのため、パスワードを使用しないこと、偽サイトに認証情報を送信できないようにすることが対策となります。パスキーは、これを実現した新しい認証方式です。

パスキーでは、利用者本人を証明する情報として、パスワードの代わりに「電子署名」というものを使います。電子署名は偽造ができない「署名・捺印」のようなものです。この電子署名はスマートフォンで作成します。加えて、電子署名を

図表2　SMSを使用した多要素認証の例



図表3　リアルタイムフィッシングの手口



第三者が勝手に作成できないようにするために、スマートフォンの生体認証（顔認証や指紋認証）で所有者の確認を行った上で電子署名を行います。また、電子署名は事前に登録した正規サイトにしか送信されないようになっています。誤って偽サイトにアクセスしても、偽サイトに電子署名が送られることはありません（**図表4**）[*3]。そのため、パスキーはリアルタイムフィッシングを含むフィッシングの対策になります。

不正ログインの被害に遭わないためのポイント（まとめ）

1. パスキーを使用したパスワードレス認証

パスキーが現時点で最も安全な認証方式であるため、パスキーが使えるサービスでは設定することを推奨します。ただし、パスキーは普及の途上にあり、すべてのサービスが対応しているわけではありません。利用しているサービスでパスキーが使えない場合は、次項の「安全なパスワードと多要素認証」を設定してください。

また、パスキーに対応しているサービスであっても、ID・パスワード認証を併用している場合があります。この場合もパスキーに加えて「安全なパスワードと多要素認証」の設定を推奨します。

2. 安全なパスワードと多要素認証の設定

「長く」、「複雑」で、複数のサービスで「使い回さない」安全なパスワードの設定を行うことを習慣にしてください。加えて、多要素認証の設定を行ってください。IPAでは、パスワードは「数字・英大文字・英小文字を組み合わせて15文字以上」にすることを推奨しています[*4]。

現状では、ID・パスワード認証も多く残っているため、安全なパスワードの設定は依然として重要です。使い回さない安全なパスワードと多要素認証を設定していれば、フィッシング等でパスワードを盗まれても、他のサービスに不正ログインされるリスクを回避できます。

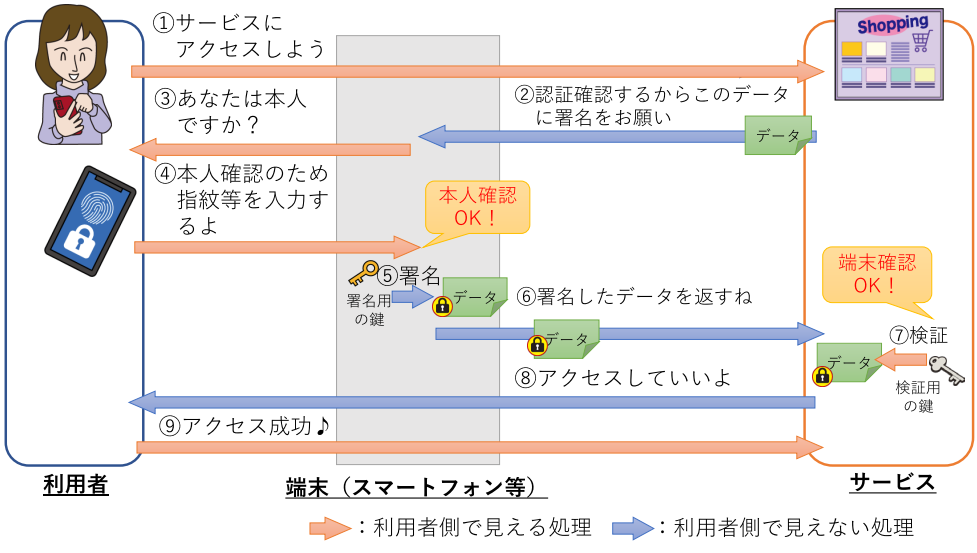
IPAでは、「長く」、「複雑」で「使い回さない」パスワードの作り方として「チョコっとプラスパスワード」という方法を提唱しています。パスワードを作る際の参考にしてください[*5]。

3. フィッシングやマルウェアに注意

フィッシングは、不正ログインにつながる最大の脅威です。また、悪意あるウェブサイトやメール等で、認証情報を盗むマルウェア（不正なプログラム）にパソコンを感染させる手口も報告されています。

こうした手口に対しては、メールの添付ファイルの開封、不審なメールやSMSのURLリンクを安易にクリックしないことが基本的な対策となります。

図表4 パスキーの概要



*3 IPA「情報セキュリティ 10大脅威2024」34ページ【パスキーとは】 https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf
*4 IPA「安心相談窓口だより：不正ログイン被害の原因となるパスワードの使い回しはNG－ちょっとした工夫でパスワードの使い回しを回避－」 https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html
*5 IPA「チョコっとプラスパスワード」 https://www.ipa.go.jp/security/chocotto/