第５回

こんなときどうしたら?
インターネットのセキュリティガイド

不正ログイン

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

本号では、「不正ログイン」について解説します。

身近に潜む不正ログインの被害

近年、インターネットを介してあらゆるコンテンツやサービスが提供されています。消費者は多様なサービスの中から、自分の好みに合ったものを利用します。そのサービスを利用するシステムの１つとして、アカウント登録が存在します。

アカウント登録は基本的にIDとパスワードを設定することで、サービスを利用する正規ユーザーの一人として認識されるしくみです。このIDとパスワードの組み合わせは正規ユーザーであると認識するための、いわば本人確認であり、そのユーザー以外は知らないことが前提です。

しかし、IDとパスワードを不正に取得した第三者が正規ユーザーになりすまし、アカウントに不正ログインする事例が多発しています。アカウントが不正ログインされると、例えばインターネット通販サービスの場合、不正に買い物をされてしまいます。

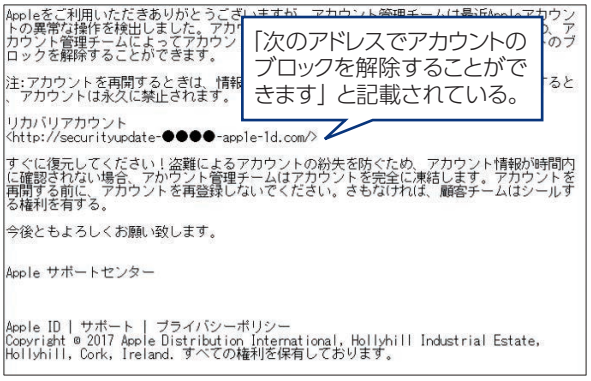
ID、パスワードが窃取される原因

では、どのような経緯でIDとパスワードが窃取されるのか、その代表例を紹介します。

■フィッシング

本連載第3回[*1]では、インターネットバンキングに限定して説明しましたが、ECサイトやSNSを対象とした手口もあります。例えば「不審なアクセスを検知しました。今すぐ確認してください」などのメールが届き、IDとパスワードを入力させるリンク先へと誘導する手口（**図1**）や、フィッシングサイトへと誘導する手口（**図2**）などです。

図１ Apple ID をねらったフィッシングメール例



資料：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」より

図２ Apple ID をねらったフィッシングサイト例

■サービス提供元からの漏えい

サービス提供元がサイバー攻撃を受けてしまい、アカウント情報（IDとパスワードのセット等）が漏えいするという事例もあります。一度漏えいしたアカウント情報は「リスト」として闇市場に出回り、別のウェブサイトへのログイン試行や次のサイバー攻撃に使うために利用されます。「リスト」を使用した攻撃を「リス

*1 ウェブ版「国民生活」2018 年９月号「こんなときどうしたら？インターネットのセキュリティガイド」第３回「偽ウェブサイトとインターネットバンキングをねらった攻撃」
http://www.kokusen.go.jp/wko/pdf/wko-201809_07.pdf

ト型攻撃」といいます。

■パスワード解析

パスワードの中には推測されやすいキーワードを使ったものがありますが、こうしたキーワードを設定した場合、推測だけでパスワードが破られる可能性があります。例えば「password」「zaqwsx（キーボードの左端2列）」や、「（名前のローマ字）＋（誕生日のような数字4桁）」のようなものです。攻撃者はこうしたよくある簡易なキーワードを事前に「辞書」としてデータ化して攻撃を行います。こうした攻撃を「辞書攻撃」といいます。

昨今のウェブサービスへの不正ログインは主にこの「リスト型攻撃」や「辞書攻撃」です。

不正ログインの被害事例

実際に起きた事例と、どのような被害に発展するかを紹介します。

1）大学で相次いだフィッシング

2018年の夏頃に複数の大学から個人情報の流出被害が確認されました[*2]。大学の学生や教職員宛てに、大学で利用しているウェブメールサービスのシステム管理者を装い「メールボックスがいっぱいです」などと書かれたフィッシングメールが送られてきたというものです。教職員などがそのメール内のリンク先にIDとパスワードを入力してしまったことが原因と考えられます。

2）フリーメールの乗っ取り

IPAには、Yahoo!メールやGmailといったフリーメールの乗っ取り被害の相談が多く寄せられます。メールアカウントが乗っ取られると、送受信履歴などから個人情報が流出してしまうだけでなく、そのアカウントで迷惑メールを送信されてしまうことが考えられます。

3）仮想通貨の不正送金

仮想通貨交換業者のウォレットに保管していた仮想通貨が、不正に送金されてしまったという被害相談もIPAに寄せられています。仮想通貨交換業者や仮想通貨を保管するウェブウォレットなどのサービスもIDとパスワードによる認証のため、前述した攻撃の方法などにより突破されたことが原因と考えられます。

4）ねらわれるキャリア決済

身に覚えのないキャリア決済があったという相談も多く寄せられています。特にApple IDからの請求だったという報告が多いです。Apple IDの支払い方法をキャリア決済に設定する際、携帯電話番号とその電話番号宛てにショートメッセージ（SMS）で送られるPINコードを入力する必要があります。何らかの方法で電話番号とPINコードが窃取されてしまうと、第三者のApple IDに勝手に連携され、不正に使用されてしまいます。

実際にフィッシングの手口で、電話番号とPINコードを盗み取ろうとする事例がありました[*3]。

不正ログインへの対策

他者に乗っ取られないためにパスワード管理などの対策が重要となります。パスワードはユーザーが任意で設定できるものです。このパスワードが安易な文字列だと、第三者に推測されてしまいます。また、パスワードを異なるサービスで使い回すことも危険です。1つのアカウントが乗っ取られた場合、使い回したパスワードを登録した他のアカウントも乗っ取られてしまい、被害がより大きくなります。

IPAが行った2017年度の意識調査[*4]によると、「パスワードは誕生日など推測されやすいものを避けて設定している」と答えた人が53.0%、「パスワードはわかりにくい文字列（8文字以上、記号含む）を設定している」が53.9%とあり、半分以上の人がパスワードを複雑にするよう意識していることが分かります。一方で、「サービス毎（ごと）に異なるパスワー

*2 日本経済新聞「6大学にフィッシングメール、1.2万件の個人情報流出」（2018年7月2日）
https://www.nikkei.com/article/DGXMZO32495350020720 18CR8000/

*3 フィッシング対策協議会「佐川急便をかたるフィッシング」（2018年8月10日）
https://www.antiphishing.jp/news/alert/sagawa_20180810.html

*4 IPA「2017年度情報セキュリティの脅威に対する意識調査」報告書
https://www.ipa.go.jp/security/fy29/reports/ishiki/index.html

ドを設定している」と答えた人は32.3%となり、7割近い人がパスワードを使い回しているという事実がうかがえます。

■安全なパスワードと管理

パスワードはできる限り「長く」「複雑」にして「使い回さない」ことが重要です。昨今の攻撃では１つのパスワードで複数のサービスに対して不正ログインを試されることが多いため、使い回した場合、複数のサービスで被害にあう可能性が高くなります。

今の時代、多くの人がさまざまなサービスアカウントを所有しています。パスワードを使い回さないようにしたくても、管理が大変になり、覚えきれなくなる不安もあると思います。

そこで、IPAでは使い回しを回避するパスワードの作成方法を紹介しています[*5]。やり方としては、すべてのパスワードに共通して使う「コアパスワード」とサービスごとに使い分ける「識別子」を組み合わせる方法です（**図3、図4**）。

この方法であれば、コアパスワードだけは暗記して、識別子だけをメモなどで記録するように管理しておけば、仮にメモを紛失した場合でも悪用される心配はありません。

図３ コアパスワード作成例

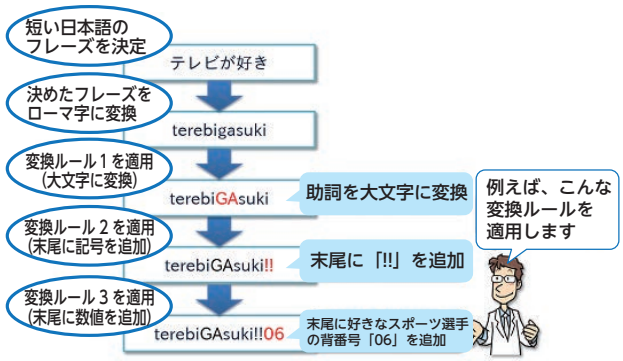


図４ 識別子作成例

■２段階認証の設定

パスワードの作成方法について解説しましたが、これに加えて2段階認証を設定することを推奨します。

認証方式には大きく分けて次の３つがあります。

認証方式	方法
記憶による認証（SYK） Something You Know	ID・パスワード、PIN認証、秘密の質問など
所有物による認証（SYH） Something You Have	SMS認証、ワンタイムパスワード、ICカード（スマートカード）など
生体認証（SYA） Something You Are	指紋認証、顔認証、静脈認証、虹彩認証など

2段階認証とはこれらの認証方式を複数組み合わせることです[*6]。パスワードに加えて、セキュリティコードの入力をさせるなどの方式で、たとえパスワードを突破されたとしても、セキュリティコードを入れなければログインできなくなるようにするしくみです。セキュリティコードが携帯電話の電話番号宛てにSMSで届くようにした場合、パスワード（SYK）とSMS認証（SYH）を組み合わせた2段階認証となります。このように、複数の認証方式を組み合わせることはセキュリティをより強固にします。

もしも、アカウントに不正ログインをされて、パスワードを勝手に変更されてしまった場合は、自分がログインできなくなります。そのような状況になった場合は、その運営会社に問い合わせることが必要になります。問い合わせの際は、そのアカウントの本来の所有者であるという証明が必要になります。運営会社によって対応は異なりますが、もし証明できない場合はアカウントを取り戻せないことも考えられます。こうしたことを想定して、事前に手続き方法などを確認しておくとよいでしょう。

大事なことは乗っ取られないことです。日頃から利用しているアカウントはいくつあり、パスワードは強固なのか、2段階認証は設定しているのかなどを確認するようにしましょう。

*5 IPA「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」
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html
*6 SYK&SYH など複数の要素を組み合わせた方式を「多要素認証」ともいう。