Information-technology
Promotion
Agency, Japan

第 13-30-297 号
2013 年 8 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 全てのインターネットサービスで異なるパスワードを！ 」
～　多くのパスワードを安全に管理するための具体策　～

パスワードリスト攻撃の被害報道が続いています（表 1 参照）。不正ログインが成立した率は低いものの、ログイン試行回数が多いほど、不正ログイン成立の実件数はかなりの数に上ってしまうことが分かります。

パスワードリスト攻撃とは、悪意のある者が、何らかの方法で事前に入手した ID とパスワードのリストを流用し、自動的に連続入力するプログラムなどを用いてそれら ID とパスワードを入力することで、ウェブサイトにログインを試みる手口です。ここでログインが成立した ID とパスワードの組み合わせはその後、他の不正アクセスに悪用され、最終的には直接金銭的被害に結びつくものと考えられます。

このような攻撃が成立する背景として、“同じパスワードを様々なインターネットサービスで使い回す利用者が多い”ということが挙げられます。パスワードリスト攻撃はこの状況に目を付けた攻撃手法と言えます。

表 1：パスワードリスト攻撃を受けたことを 2013 年 4 月以降公表した企業のうち、「試行件数」と「成立件数」の両方が公表された主なもの

被害企業	不正ログインの試行件数（A）	不正ログインの成立件数（B）	不正ログイン成立率※（B/A）
A 社	約 24,000	77	0.32%
B 社	約 26,000	97	0.37%
C 社	約 1,110,000	約 15,000	1.35%
D 社	約 240,000	682	0.28%
E 社	5,202,002	8,289	0.16%
F 社	11,031	126	1.14%
G 社	15,457,485	23,926	0.15%
H 社	3,945,927	35,252	0.89%

※「不正ログイン成立率」は、企業が公表した数値（A および B）を基に、IPA が算出したものです。

大規模なパスワードリスト攻撃は大きく取り上げられる傾向にありますが、それらは氷山の一角である可能性があります。自分の使っているインターネットサービスではパスワードリスト攻撃の被害の報告がないからと言っても決して安心はできません。

最近では個人が利用するインターネットサービス（サイト）の数が増加しており、パスワードを覚え切れないからと言ってつい使い回ししがちです。しかし「パスワードを使い回ししないように」と言われても、覚え切れないパスワードを実際にどうしたらいいか分からない利用者も多いのではないでしょうか。

今回の呼びかけでは、多くのパスワードを安全に管理した上で、個人の利用者がパスワードの使い回しを避ける具体的な方法について説明します。

(1) パスワードリスト攻撃の手口

インターネットサービスの利用者の多くが複数サイトで同一の ID とパスワードを使い回している状況に目をつけ、不正取得した ID とパスワードのリストを流用し、連続自動入力プログラムなどを用いて ID とパスワードを入力しウェブサイトへのログインを試行する手口です。（図 1 参照）

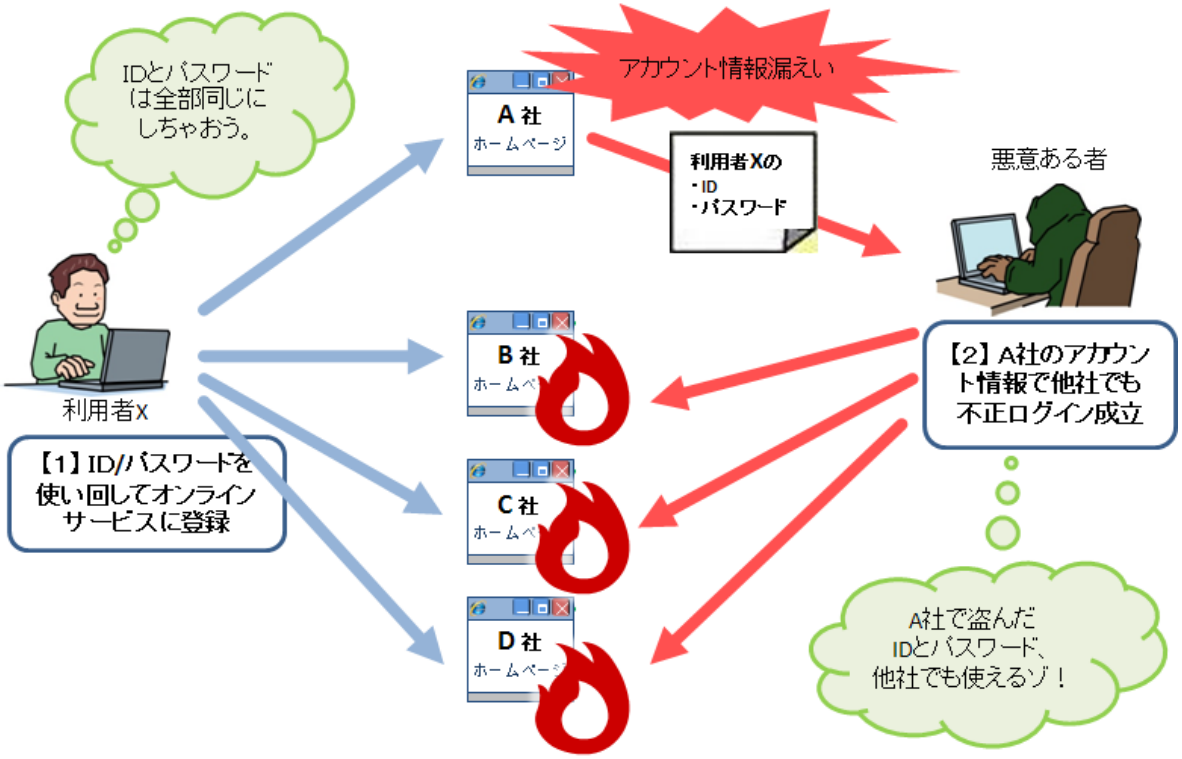

図 1：利用者の観点から見た、パスワードリスト攻撃による被害のイメージ図

図中【1】のように、各社のサービスにおいて ID とパスワードをすべて同じにしている場合、その中のいずれかのサービス企業でアカウント情報が漏えいしてしまうと、図中【2】のように悪意ある者が他社のサービスで同じ ID とパスワードを用いて、利用者 X になりすましてログインすることができます。これで、パスワードリスト攻撃が成功したことになります。その後、悪意ある者はログイン可能な ID とパスワードを悪用して不正アクセスし、最終的には金銭に結びつくような二次的被害を引き起こします。

ここで注意すべき点は、パスワードリスト攻撃においては、その元となる ID とパスワードは、個人のパソコンからではなくインターネットサービスのサーバーから盗み取られる、ということです。

つまり、**利用者側で強固なパスワードを設定し、かつパソコン上でセキュリティソフトを利用していても、同一のパスワードを使い回している限り、パスワードリスト攻撃の被害を防ぐことはできません**。

(2) パスワードの使い回しを避け、安全に管理するための具体策の例

個人の利用者が**パスワードリスト攻撃による最終的な被害者にならないようにするためには、すべてのインターネットサービスで異なるパスワードを設定する必要があります**。

そして、すべてのサービスで異なるパスワードを設定し、それらを日常的に利用するためには、**“複数のパスワードを”、“どのように管理するか”が重要**となります。そのための具体策を以下に示します。

① 自分が利用する ID とパスワードを、リスト化して保持

多くのサービスで異なるパスワードを設定していると、すべての ID とパスワードを暗記することは困難で、何らかの形でリストとして保持することが現実的な解となります。

紙のノートやメモ帳などに保持していても良いのですが、リストが肥大化した際のメンテナンス性を考慮し、ID とパスワードを記載したリストを**「パスワード付きの電子ファイル」**として保持することを勧めます。

具体的には、

・表計算ソフトで ID とパスワードのリストを作成する。そのリストを、パスワード付きでファイル保存する。

・表計算ソフトで ID とパスワードのリストを作成し、ファイル保存する。そのファイルを、パスワード付きで圧縮ファイル（zip など）に変換する。

・「メモ帳」などで ID とパスワードのリストを作成し、テキストファイルとして保存する。そのファイルを、パスワード付きで圧縮ファイルに変換する。

などの方法があります。

② サービスの重要度によっては、ID とパスワードのリストを別々のファイルに分けて保持

インターネットバンキングの ID とパスワードなど、金銭に絡む重要なものについては、上記①リストを用いた管理に加え、ID とパスワードを切り離して保持することを勧めます。

	ID	サービス名
1	aaaaa	○×銀行
2	bbbbb	△○銀行
3	ccccc	▼○証券
4	ddddd	△×オンラインショップ
:	:	:
:	:	:

	パスワード
1	4gs2FWo3qq
2	RF3jfei3ie
3	0p88jIssJF2
4	JWw24g13mn
:	:
:	:

図 2：ID とパスワードを別々に保持するイメージ図

図 2 の左は、「ID」と「サービス名」のリスト、図 2 の右は「パスワード」のリストです。

この 2 つのリストを普段から別々に保持します（例：パソコンと紙、パソコンとスマートフォン、など）。もし片方を盗み取られても、それだけでは不正ログインに悪用することができないため安全です。

例えば○×銀行にログインする場合には、各リストの「1」の列を見て、ID とパスワードをそれぞれ読み取ります。

もし ID を覚えている場合は、ログイン時に図 2 右のパスワードのリストだけを見れば良いことになります。

(3) 実際に被害が発生した時の、事後対処について

不正ログインの被害に遭ったことが判明した場合、可能であれば、さらなる被害を防ぐために、パスワードをすぐに変更してください。その上で、サービス会社のサポート窓口に連絡し、実被害が生じた場合の補償や今後の対応について説明を受けてください。

また、不正ログインされた ID の決済情報としてクレジットカードが紐付いている場合は不正利用される恐れがあるため、クレジットカード会社の窓口にも連絡してください。万が一、クレジットカードが不正利用されても補償される可能性が高いですが、速やかにクレジットカード会社に連絡を取り、対処方法について相談することを勧めます。

■お問い合わせ先
IPA 技術本部セキュリティセンター 加賀谷／田中
Tel:03-5978-7591 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp