第 15-10-335 号
2015 年 7 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 その秘密の質問の答えは第三者に推測されてしまうかもしれません 」

「秘密の質問」とは、「質問」とそれに対応する本人しか知らない「答え」を設定し、パスワードリマインダやインターネットバンキングでの本人を確認するための機能です。例えば、パスワードリマインダで利用する場合、あらかじめ「質問」と「答え」を設定しておくことで、パスワードを忘れた際には「秘密の質問」によって本人確認をします。しかし、**「秘密の質問」のみで本人確認とすることにはセキュリティ上の懸念があります**。

2015 年 5 月、Google 社が「秘密の質問」に関する研究結果を発表したことが報じられました※1。それによると、「秘密の質問は、それ単体でアカウント復旧の仕組みとして使用するには、安全性も信頼性も十分ではない」とされています。

2014 年 9 月には、iCloud に保存されていた米国人気女優やモデルなど著名人のプライベート画像が多数流出した件で、Apple 社が調査状況を公表※2しました。それによると、「ユーザ名、パスワード、セキュリティーのための質問を対象とした非常に的を絞った攻撃」によってアカウントが乗っ取られてしまったことが明らかにされており、「秘密の質問」も狙われたと考えられます。

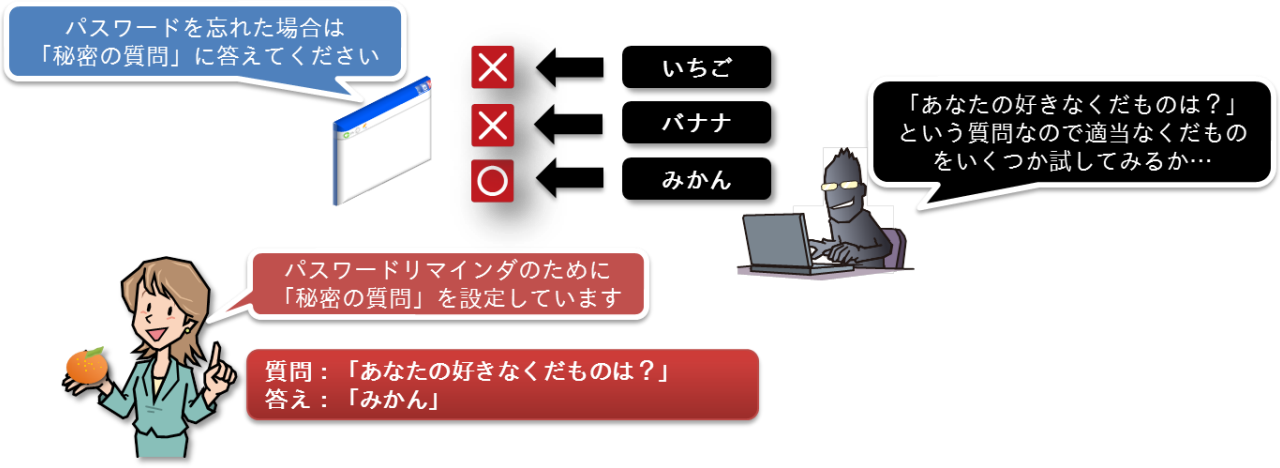

図 1：「秘密の質問」が攻撃の対象となることも

また、サービスの仕様にもよりますが、パスワードリマインダを使用した際に「秘密の質問」のみによる本人確認後、画面にパスワードがそのまま表示されることもあります。この場合、第三者

[1] ZDNet Japan：パスワードを忘れた時の「秘密の質問」、あまり安全ではない？--グーグル調査
http://japan.zdnet.com/article/35065000/
[2] Apple：著名人の写真に関する調査状況の報告
https://www.apple.com/jp/pr/library/2014/09/02Apple-Media-Advisory.html

に「秘密の質問」の「答え」を当てられるとパスワードを知られてしまうことになり、不正にサービスを利用されるなどの被害に繋がる恐れもあります。そのため、利用者は「秘密の質問」以外にサービスが提供している本人確認の方法を確認し、提供されている場合は、別の方法への変更または併用を検討する必要があります。

今月の呼びかけでは、この「秘密の質問」を利用する上での注意点と、利用者に推奨する対策およびサービス提供者に求められること、について紹介します。

（1） 「秘密の質問」の注意点

サービス提供者があらかじめ用意している「質問」のなかから利用者が選択するのが一般的で、例えば「あなたの母親の旧姓は？」「あなたのペットの名前は？」などがあり、利用者はそれに対応する「答え」を設定します（図 2）。

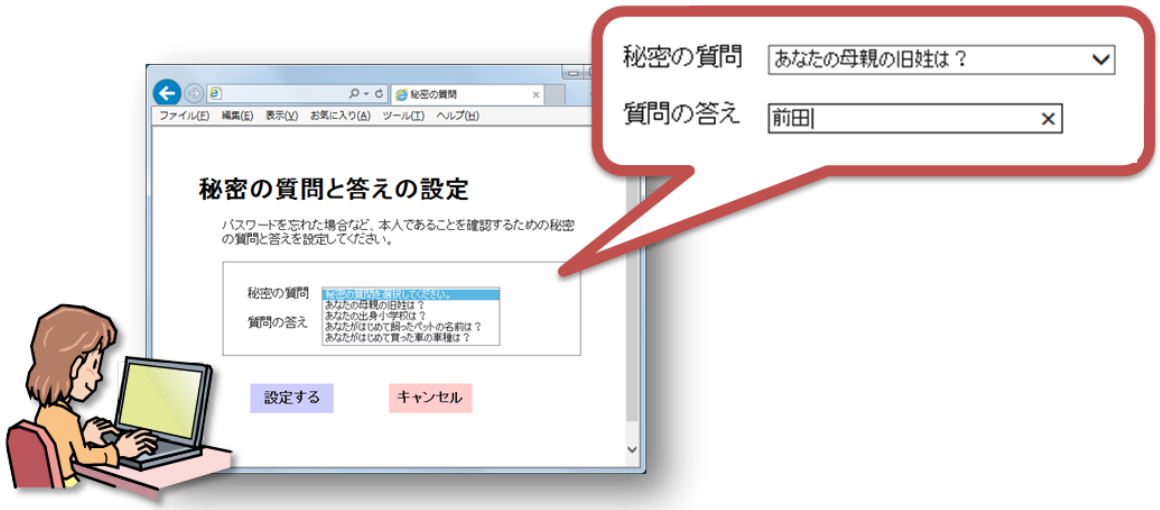

図 2：「質問」と「答え」の設定画面（イメージ）

「秘密の質問」では事前に設定した「質問」に対応する「答え」を入力するだけで本人確認ができるため便利です。しかし、「質問」によっては、第三者でも「答え」を推測できてしまう場合があります。

例えば「あなたの母親の旧姓は？」という「質問」の場合、「答え」には姓が設定されていると推測することができます。このため、悪意ある第三者が「佐藤」や「鈴木」などのよくある姓で入力を繰り返すと、「答え」を当ててしまう可能性があります。また、「あなたのペットの名前は？」という「質問」の場合も、ペットの名前ランキングを調べたり、本人の SNS でペットの名前が公開されていないかを調べるなどの方法で「答え」を推測することも考えられます。

前述のように「秘密の質問」への「答え」の入力だけで本人確認ができてしまうと、パスワードを不正に入手される可能性もあるため、**「秘密の質問」の「答え」はパスワードと同じように第三者に推測されにくい内容にする必要があります。**

（2） 利用者に推奨する対策

まず、利用しているサービスにおいて「秘密の質問」の設定の有無を確認してください。

また利用しているサービスが「秘密の質問」以外に、ワンタイムパスワードによる二段階認証など、複数の本人確認方法を提供しているかを確認してください。複数ある場合は「秘密の質問」以外の方法に変更、または併用を検討してください。

さらに「答え」は第三者に推測されにくい内容への変更も検討してください。しかし、「答え」を複雑な内容にすると、本人が思い出せなくなる可能性が懸念されます。

そこで、IPA では図 3 に示すように**“「本来の答え」に自分しか知らない「共通フレーズ」を追加”**して、第三者に推測されにくい「答え」とすることを推奨します。

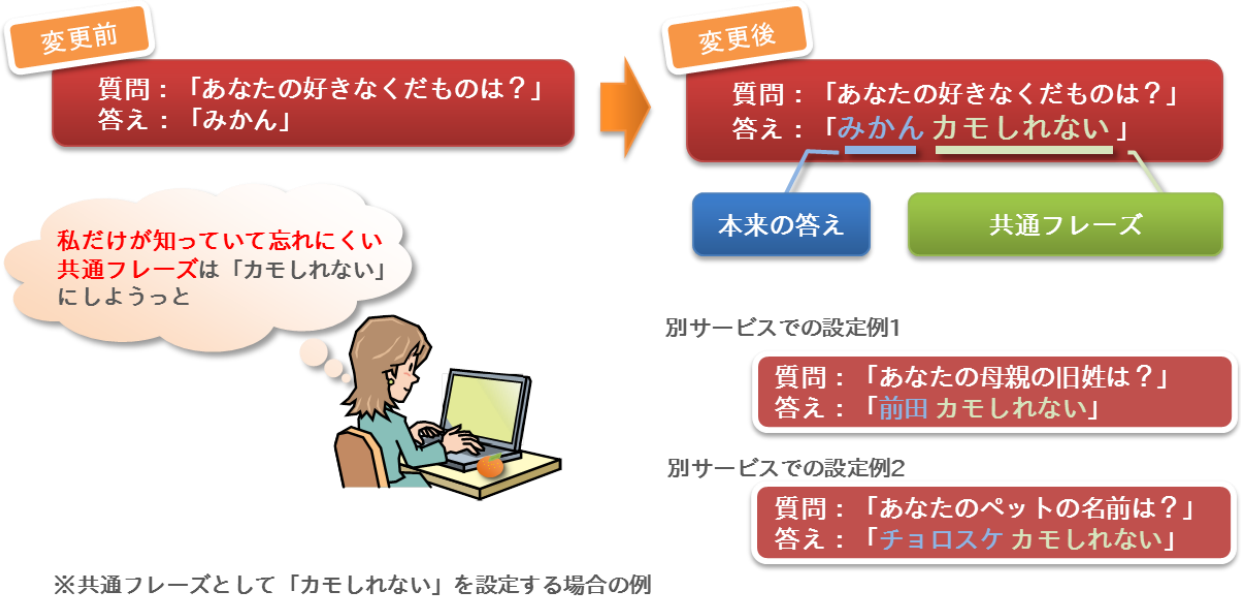

図 3：第三者に推測されにくい「答え」の設定例

「共通フレーズ」として自分しか知らない文字列を設定することで、文字数や文字種を増やすことができ、第三者から推測される可能性を減らすことができます。ただし、異なるサービスで同じ「質問」を選択した場合、推測されにくいとは言え「答え」が同じになります。このような場合は、「サービス毎に異なる識別情報」として、更にサービス名の一部を加えて「みかん カモしれない アイピイエイ」（ここでは「アイピイエイ」が識別情報）などとする方法もあります。

（3） サービス提供者に求められること

サービス提供者には、利用者が「秘密の質問」を安全に利用できるための配慮が求められます。具体的には**「秘密の質問」だけで本人確認が完了とならないように、ワンタイムパスワードによる二段階認証など、複数の本人確認方法を用意し、利用者が選択や変更、あるいは併用できるようなサービスを提供すること**です。

また、「秘密の質問」による本人確認のセキュリティレベルを向上させるため、以下のような対策を検討してください。

■「質問」の内容から第三者に「答え」を特定されないための対策
・利用者が設定した「質問」はいつでも変更できるようにする
・利用者が「質問」を自由に記述できるようにする
・万が一の漏えいに備えて設定された「質問」は暗号化して管理する

■「答え」を第三者に推測されないための対策
・利用者が設定した「答え」はいつでも変更できるようにする
・利用者が「答え」で設定できる文字数や文字種を可能な限り増やす
・万が一の漏えいに備えて設定された「答え」はソルト付きハッシュ値※3として管理する

■お問い合わせ先
情報セキュリティ安心相談窓口
Tel: 03-5978-7509　Fax: 03-5978-7518
E-mail: anshin@ipa.go.jp
技術本部セキュリティセンター 加賀谷／野澤

[3] ソルト付きハッシュ値：ハッシュの元となるデータに、ソルトと呼ばれる利用者毎に異なる値で生成した文字列をつなげてハッシュ化した値。